INFORME DE VERIFICACIÓN DEL CUMPLIMIENTO DE LA NTC ISO/IEC 27001:2022 MEDIANTE EL SEGUIMIENTO AL AVANCE DEL PLAN DE MEJORAMIENTO INSTITUCIONAL – VIGENCIA 2026							
FECHA DE EMISIÓN DEL INFORME	**Día:**	07	**Mes:**	0	7	**Año:**	2026

Contenido

1. Introducción

En cumplimiento de las funciones de evaluación y seguimiento establecidas en la Ley 87 de 1993 y de las actividades programadas en el Plan Anual de Auditoría Basada en Riesgos para la vigencia 2026, la Oficina de Control Interno realizó la verificación del cumplimiento de la Norma Técnica Colombiana NTC ISO/IEC 27001:2022, mediante el seguimiento al avance de las acciones de mejoramiento formuladas como resultado de la auditoría de cumplimiento efectuada durante la vigencia 2025.

La presente actividad tiene como finalidad determinar el estado de avance de las acciones implementadas por la entidad y evidenciar los progresos alcanzados en el fortalecimiento de la gestión de la seguridad de la información, así como identificar los avances obtenidos en el cumplimiento de los requisitos establecidos en la Norma Técnica Colombiana NTC ISO/IEC 27001:2022, considerando que las actividades definidas en el plan de mejoramiento continúan dentro de los plazos previstos para su ejecución.

2. Objetivo

Verificar el avance de las acciones de mejoramiento formuladas como resultado de la auditoría de cumplimiento a la Norma Técnica Colombiana NTC ISO/IEC 27001:2022, realizada durante la vigencia 2025, con el fin de determinar los progresos alcanzados y el grado de cumplimiento de los requisitos establecidos en dicha norma por parte de la Corporación Autónoma Regional del Magdalena – CORPAMAG.

3. Alcance

El seguimiento comprendió las acciones de mejoramiento formuladas como resultado de la auditoría de cumplimiento a la Norma Técnica Colombiana NTC ISO/IEC 27001:2022 realizada durante la vigencia 2025, cuyo plazo de ejecución se encuentra vigente durante el año 2026.

Los aspectos objeto de seguimiento se encuentran relacionados con la seguridad y privacidad de la información, la continuidad del negocio, la gestión de riesgos, la arquitectura empresarial, la interoperabilidad, la adopción del protocolo IPv6, el uso de datos, los datos abiertos y la disposición de trámites y servicios digitales, de acuerdo con los temas evaluados en la auditoría y los compromisos definidos en el plan de mejoramiento institucional.

4. Criterios

- Ley 87 de 1993 "Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones".

- Norma Técnica Colombiana NTC 27001:2022 del 25 de octubre de 2022 “Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos”.

- Decreto 767 de 2022. Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Resolución 02277 de 2025 del Ministerio de Tecnologías de la Información y las Comunicaciones “Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia”.

- Resolución 1519 de 2020 del Ministerio de Tecnologías de la Información y las Comunicaciones “Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 de 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos”.

5. Limitaciones del seguimiento

Durante el desarrollo del presente seguimiento se presentaron limitaciones relacionadas con la oportunidad en la remisión de la información y evidencias requeridas por la Oficina de Control Interno.

Si bien la actividad de seguimiento se encontraba programada para el mes de junio de 2026, la entrega extemporánea de la información por parte del Grupo de Tecnologías de la Información y las Comunicaciones (TIC) hizo necesaria la emisión de solicitudes reiterativas para completar la documentación requerida, situación que conllevó a que la consolidación y emisión del presente informe se efectuara durante el mes de julio de 2026.

6. Equipo Auditor

Contratista: Luz Piedad Echavarría López
Supervisión del trabajo: Liliana Hidalgo García, Jefe Oficina de Control Interno

7. Metodología

La verificación se desarrolló mediante la solicitud y revisión de información, el análisis de los soportes documentales aportados y la aplicación de técnicas de auditoría orientadas a obtener evidencia suficiente y adecuada que permitiera determinar el avance de las acciones de mejoramiento formuladas y su contribución al cumplimiento de los requisitos establecidos en la Norma Técnica Colombiana NTC ISO/IEC 27001:2022.

1. Inspección

Consistió en el examen de los documentos, registros y demás evidencias aportadas por el Grupo de Tecnologías de la Información y las Comunicaciones (TIC), con el propósito de verificar el avance de las actividades formuladas en el plan de mejoramiento institucional y su contribución al cumplimiento de los requisitos de la Norma Técnica Colombiana NTC ISO/IEC 27001:2022.

2. Observación

Verificación selectiva de la información publicada en el sitio web institucional y demás plataformas oficiales, así como de las condiciones reportadas por el auditado, cuando se consideró necesario para corroborar la información suministrada.

3. Procedimientos analíticos

Consistieron en el análisis y comparación de la información y evidencias aportadas frente a las actividades definidas en el plan de mejoramiento institucional y los requisitos normativos aplicables, con el fin de identificar avances, inconsistencias y aspectos pendientes de implementación relacionados con el cumplimiento de la Norma Técnica Colombiana NTC ISO/IEC 27001:2022 por parte de la Corporación Autónoma Regional del Magdalena – CORPAMAG.

8. Resultados de la verificación

La revisión efectuada se orientó a verificar el estado de implementación de las acciones formuladas por la entidad, la suficiencia de las evidencias aportadas y la manera en que las medidas adoptadas contribuyen al fortalecimiento de la gestión de la seguridad de la información y al cumplimiento progresivo de los requisitos establecidos en la Norma Técnica Colombiana NTC ISO/IEC 27001:2022 y de los lineamientos asociados a la Política de Gobierno Digital.

Los resultados detallados del seguimiento se presentan a continuación:

Tabla 1 seguimiento del estado de avance del plan de mejoramiento y su contribución al fortalecimiento del cumplimiento de la NTC ISO/IEC 27001:2022.

Descripción del hallazgo	Acción de mejora	Estado	Resultado del seguimiento
Al revisar la evidencia entregada correspondiente al test normativo elaborado bajo la versión ISO/IEC 27001:2013, se constató que el documento relaciona los controles del Anexo A, su estado, observaciones y recomendaciones. El auditado dejó explícito que la Declaración de Aplicabilidad no ha sido actualizada conforme a la versión vigente ISO/IEC 27001:2022, y que se proyecta su actualización institucional. Durante la verificación del test normativo, se identificaron anotaciones de mejora y controles no implementados, algunos de los cuales están determinados por normatividad vigente en Colombia, por lo que su cumplimiento no es opcional.	Actualización del test de autodiagnóstico Anexo A de la norma ISO 27000:2013 (114 Controles) a ISO 27000:2022 (94 Controles)	Se está trabajando en la plantilla oficial actualizada suministrada por el MinTIC. El diligenciamiento se adelanta de forma progresiva conforme a los cuatro dominios de la nueva estructura normativa (Organizacionales, Personas, Físicos y Tecnológicos).	Como parte del seguimiento al plan de mejoramiento, se revisó el avance de la actualización del autodiagnóstico del Anexo A de la NTC ISO/IEC 27001:2022, evidenciando que la Corporación adelanta su diligenciamiento utilizando el formato oficial dispuesto por el MinTIC. La documentación aportada incorpora información correspondiente a los dominios Organizacionales, Personas, Físicos y Tecnológicos, en concordancia con la estructura establecida en la versión 2022 de la norma. La acción de mejoramiento continúa dentro del plazo previsto para su ejecución.
La entidad cuenta con políticas de seguridad de la información formalmente adoptadas mediante la Resolución 5846 del 28 de diciembre de 2021, en la cual se aprueba el Modelo de Seguridad y Privacidad de la Información (MSPI), la Política General de Seguridad y Privacidad de la Información y la Política de Seguridad Digital de CORPAMAG. Se evidenció su socialización interna y se aportaron documentos complementarios como el Manual de Políticas 2025 y una circular institucional sin fecha ni firma. Sin embargo, la política vigente fue formulada bajo lineamientos anteriores a la versión ISO/IEC 27001:2022 y no se evidenció documentación técnica que respalde el proceso de actualización anunciado. Este aspecto está regulado por el artículo 2.2.17.4.3, numeral 7, del Decreto 1078 de 2015, modificado por el Decreto 620 de 2020, y actualizado por la Resolución 02277 del 3 de junio de 2025, que establece los lineamientos técnicos vigentes para el Modelo de Seguridad y Privacidad de la Información como habilitador del Gobierno Digital.	Gestionar la formalización y puesta en vigencia del Manual de Políticas de Seguridad y Privacidad de la Información de CORPAMAG 2025, mediante la emisión del acto administrativo de aprobación por parte de la Alta Dirección, asegurando su publicación, divulgación interna y registro de trazabilidad conforme a los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma ISO/IEC 27001:2022.	Se cuenta con el documento de Políticas de Seguridad y Privacidad de la Información, el Manual correspondiente y el proyecto de resolución de adopción debidamente redactado. El paso siguiente es su presentación ante el Comité Institucional para aprobación y posterior emisión del acto administrativo.	La evidencia aportada para esta acción de mejoramiento corresponde a la actualización del Manual de Políticas de Seguridad y Privacidad de la Información, estructurado conforme a la NTC ISO/IEC 27001:2022 y a los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI). Asimismo, se aportó el proyecto de resolución para la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) y de las Políticas de Seguridad y Privacidad de la Información, lo que evidencia el avance en las actividades orientadas a su formalización institucional, conforme a lo previsto en la acción de mejoramiento.
Se observó que la entidad mantiene un inventario vigente y estructurado de activos de información, que incluye activos físicos (equipos de cómputo, impresoras, dispositivos de red), activos digitales (aplicativos, bases de datos, sistemas de información), activos documentales (listados de datos, formatos, archivos institucionales) y activos de soporte (infraestructura tecnológica). El inventario presenta clasificación por tipo y nivel de criticidad, asignación de responsables por activo y controles de protección definidos, conforme a lo establecido en el Modelo de Seguridad y Privacidad de la Información (MSPI). La entidad señala que los responsables pueden	Se debe implementar un procedimiento formal para actualizar periódicamente el inventario de activos de información, siguiendo el MSPI. Este procedimiento debe incluirá: Frecuencias de revisión definida, Responsables del proceso claramente asignados, Flujos de aprobación establecidos y Mecanismos de	Se ha diseñado y elaborado la plantilla de control del inventario de activos de información, la cual incorpora los elementos requeridos: frecuencias de revisión, responsables asignados, flujos de aprobación y mecanismos de evidencia documental. Se avanza en su implementación formal dentro del MSPI.	Para soportar el avance de esta acción de mejoramiento, se revisó la evidencia aportada, correspondiente al Formato de Inventario de Activos de Información, el procedimiento de Actualización del Inventario de Activos de Información y el documento "Inventario de Activos de Información – CORPAMAG". La documentación evidencia la estructuración del procedimiento para la gestión y actualización del inventario de activos de información, incorporando la frecuencia de revisión, la asignación de responsables, los flujos de aprobación y

Descripción del hallazgo	Acción de mejora	Estado	Resultado del seguimiento
variar debido a la movilidad de cargos, lo cual requiere mecanismos de actualización periódica para garantizar la trazabilidad y la vigencia de las asignaciones.	evidencia documentados. Esto con el Objetivo: Mantener la trazabilidad, vigencia de responsables, integridad y confiabilidad del inventario institucional.		los mecanismos de soporte documental, previstos en la acción de mejoramiento.
Se evidenció que la entidad cuenta con el Manual de Políticas de Seguridad y Privacidad de la Información CORPAMAG 2025, en el cual se definen lineamientos generales para el uso de técnicas criptográficas en la protección de información sensible, en concordancia con el modelo de gestión de seguridad de la información. En la respuesta entregada, se indicó que los servicios de correo electrónico corporativo en Microsoft 365 emplean cifrado en tránsito y en reposo, y que la base de datos Oracle utilizada por el proveedor implementa mecanismos nativos de cifrado para la protección de la información. Sin embargo, no se presentaron evidencias que respalden el uso de criptografía en archivos, comunicaciones, dispositivos o respaldos, conforme a lo definido en la política institucional y a los controles exigibles por la Ley 1581 de 2012, el Modelo de Seguridad y Privacidad de la Información (MSPI) y los lineamientos técnicos actualizados por la Resolución 02277 de 2025. Adicionalmente, no se indica si todas las bases de datos utilizadas por la entidad corresponden a tecnología Oracle, por lo que en caso de existir otras plataformas, estas podrían no cumplir con los mecanismos de cifrado declarados, afectando la trazabilidad y cobertura del control.	Realizar una revisión técnica y normativa de los mecanismos criptográficos implementados, identificar las brechas frente a lo definido en el Manual de Políticas de Seguridad y Privacidad de la Información CORPAMAG 2025	Los sistemas de información de terceros utilizados por CORPAMAG gestionan sus propios esquemas de cifrado bajo la responsabilidad de cada proveedor. En cuanto al desarrollo interno, el sistema de gestión de tickets y mesa de ayuda actualmente en desarrollo cuenta con su arquitectura criptográfica documentada, garantizando la seguridad en el manejo de la información.	La documentación aportada para esta acción de mejoramiento comprende la revisión de los mecanismos criptográficos implementados por la Corporación, así como una matriz que identifica los aspectos por fortalecer para la protección de la información institucional. Adicionalmente, el auditado manifestó que los sistemas de información administrados por terceros gestionan sus propios mecanismos criptográficos bajo la responsabilidad de cada proveedor, mientras que para el Sistema de Tickets y Encuestas, desarrollado por la entidad, se documentaron los controles de seguridad y criptografía implementados. La evidencia revisada refleja el avance en la identificación y documentación de los mecanismos criptográficos asociados a los sistemas de información institucionales.
Se verificó que la entidad cuenta con servicios de vigilancia y control de acceso físico conforme al contrato MC 004-2025, incluyendo circuito cerrado de televisión, control biométrico y custodia del cuarto de servidores bajo llave. Estas medidas permiten mitigar riesgos de accesos no autorizados, daños o interferencias sobre los activos tecnológicos críticos. Sin embargo, se observó que el centro de cableado no cuenta con medidas de seguridad física equivalentes, y que tanto este espacio como el cuarto de servidores presentan niveles de humedad que podrían afectar la infraestructura tecnológica.	Implementar controles físicos equivalentes en el centro de cableado y realizar las adecuaciones necesarias para eliminar las humedades en este espacio y en el cuarto de servidores, garantizando la protección de los activos tecnológicos conforme al Modelo de Seguridad y Privacidad de la Información del Gobierno Digital.	El cuarto de servidores tiene el problema de humedad completamente solucionado y el acceso se encuentra restringido exclusivamente al personal de infraestructura. Respecto al centro de cableado, se presentará recomendación formal para el traslado de los interruptores eléctricos del patio, de forma que el espacio pueda asegurarse con llave, cuyo acceso quedará bajo control del personal de seguridad y del responsable de infraestructura.	Se revisó la evidencia presentada para soportar el avance reportado, correspondiente a dos memorandos relacionados con las acciones adelantadas para atender las condiciones de seguridad física del cuarto de servidores. Durante la revisión se evidenció que los memorandos aportados carecen de las firmas que permitan acreditar su formalización. Asimismo, en el soporte de ejecución el auditado informó que el problema de humedad del cuarto de servidores fue completamente solucionado; sin embargo, en visita de verificación realizada por la Oficina de Control Interno, respaldada con registro fotográfico, se constató que dicha condición persiste, por lo que no fue posible corroborar la eliminación de la humedad informada por el auditado. En consideración a que la acción de mejoramiento se encuentra dentro del

Descripción del hallazgo	Acción de mejora	Estado	Resultado del seguimiento
			plazo establecido para su ejecución, esta continuará siendo objeto de seguimiento en las próximas verificaciones.
La entidad cuenta con un Plan de Mantenimiento Preventivo 2025 formalmente establecido, respaldado por el Contrato CD 200 de 2025, que contempla mantenimiento preventivo y correctivo de equipos tecnológicos. Se verificó su ejecución mediante los formatos FR.GT.003 y Solicitud de soporte TIC. En cuanto a respaldos, se evidenció que la información se almacena en la Nube Privada de CORPAMAG (Synology Drive) y se realiza copia nocturna automatizada a Dropbox, conforme a la configuración validada en Cloud Sync. Esta evidencia permite confirmar la existencia de controles periódicos de respaldo y mantenimiento, aunque no se aportaron bitácoras de cambios ni pruebas de restauración documentadas.	Documentar formalmente las bitácoras de cambios y configuraciones de los sistemas tecnológicos, y realizar pruebas periódicas de restauración de respaldos, garantizando la trazabilidad y disponibilidad de la información conforme al Modelo de Seguridad y Privacidad de la Información del Gobierno Digital.	Se ha diseñado la bitácora formal para el control de cambios y configuraciones de los sistemas tecnológicos. Se avanza en su implementación y en la definición del esquema de pruebas periódicas de restauración de respaldos.	Se evidenció la elaboración del documento GSI-PR-007 "Bitácora de Cambios Tecnológicos y Pruebas de Restauración de Respaldos", el cual establece el procedimiento propuesto para el registro de cambios tecnológicos, la ejecución de pruebas de restauración de respaldos, los formatos de registro, el cronograma y los indicadores de seguimiento. Asimismo, se aportó el Plan de Mantenimiento Preventivo de Infraestructura TIC 2026.
Se comprobó que la entidad incluye medidas de seguridad de la información en los contratos suscritos con proveedores que acceden, procesan o almacenan información institucional. En el contrato 053 de 2025 con la empresa XENCO S.A se evidencian cláusulas específicas sobre: - Confidencialidad de la información institucional (Cláusulas 14 y 33) - Restricciones de acceso a datos y sistemas (Cláusulas 30 y 31) - Obligaciones de protección de datos personales conforme a la Ley 1581 de 2012 y el Decreto 1377 de 2013 (Cláusula 32) - Propiedad exclusiva de la información por parte de CORPAMAG, con derecho a copias de seguridad diarias y auditoría de cumplimiento - Compromiso de no divulgación ni uso indebido de la información institucional por parte del proveedor Estas cláusulas permiten validar el cumplimiento de los controles exigibles por el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Resolución 02277 de 2025. No se recibió evidencia de evaluación de proveedores.	Diseñar y aplicar un procedimiento formal para la evaluación técnica y de riesgos de los proveedores que acceden o procesan información institucional, incorporando criterios de cumplimiento en seguridad de la información, trazabilidad contractual y verificación de controles, conforme a los lineamientos del MSPI y los controles A.5.19 y A.5.20 de la norma ISO/IEC 27001:2022.		A la fecha del seguimiento no se aportó evidencia que permita corroborar avances en el diseño y documentación del procedimiento formal para la evaluación técnica y de riesgos de proveedores. No obstante, las actividades previstas continúan dentro del plazo establecido para su ejecución, por lo que la acción permanecerá abierta y continuará siendo objeto de seguimiento.
Se evidenció que la entidad cuenta con el procedimiento PR.GT.004 Gestión de la Seguridad de la Información, el formato institucional “16 - Registro de Incidentes de Seguridad de la Información” y documentación técnica del incidente ocurrido en 2024, lo cual permite validar la aplicación de controles relacionados con la preparación, respuesta y registro de incidentes. El procedimiento contempla las fases de identificación, reporte, análisis y respuesta, incluyendo la asignación de responsabilidades y	Actualizar el procedimiento PR.GT.004 Gestión de la Seguridad de la Información para garantizar su alineación con la normatividad vigente (Decreto 620 de 2020 y Resolución 02277 de 2025), el Modelo de Seguridad y Privacidad de la Información (MSPI) y los controles A.5.25,		A la fecha del seguimiento no se aportó evidencia que permita corroborar la actualización del procedimiento PR.GT.004 conforme a los lineamientos establecidos en el Decreto 620 de 2020, la Resolución 02277 de 2025 y la NTC ISO/IEC 27001:2022. No obstante, las actividades continúan dentro del plazo previsto para su ejecución..

Descripción del hallazgo	Acción de mejora	Estado	Resultado del seguimiento
los mecanismos de seguimiento de los eventos reportados. Esta práctica se encuentra alineada con los controles A.5.25, A.5.26 y A.5.27 de la NTC ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información (MSPI) y los lineamientos del Gobierno Digital establecidos en el Decreto 620 de 2020.	A.5.26 y A.5.27 de la ISO/IEC 27001:2022, asegurando su aplicación frente a nuevos escenarios de riesgo.		
Se analizó el documento "Plan de Continuidad del Negocio – CORPAMAG 2025", el cual contempla de manera explícita las medidas específicas de seguridad de la información necesarias para garantizar la protección de datos y la disponibilidad de los servicios críticos ante interrupciones o emergencias. El plan incluye: - Análisis de impacto al negocio (BIA) y evaluación de riesgos - Estrategias de respaldo y recuperación tecnológica (DRP), incluyendo respaldos diarios, nube híbrida y definición de RTO/RPO - Identificación de procesos críticos misionales, de apoyo y estratégicos - Comité de crisis con funciones definidas y roles asignados - Canales de comunicación internos y externos, con vocería oficial Estas medidas están alineadas con los controles A.5.29 y A.5.30 de la NTC ISO/IEC 27001:2022, la NTC ISO 22301:2012, el Decreto 620 de 2020 y los lineamientos del Modelo de Seguridad y Privacidad de la Información del Gobierno Digital. El documento se encuentra en versión redactada y aún no ha sido aprobado formalmente por la alta dirección, lo cual limita su oficialización, divulgación institucional y aplicación operativa.	Gestionar la aprobación formal del Plan de Continuidad del Negocio (PCN) por parte de la Alta Dirección mediante resolución, garantizando su oficialización, divulgación y aplicación operativa conforme al Decreto 620 de 2020, la Resolución 02277 de 2025 y las normas ISO/IEC 27001:2022 e ISO 22301:2012.	Se cuenta con la redacción completa del Plan de Continuidad del Negocio (PCN) y del Plan de Recuperación ante Desastres (DRP), ambos listos para ser presentados ante el Comité Institucional para su aprobación y posterior formalización mediante resolución, conforme al Decreto 620 de 2020, la Resolución 02277 de 2025 y las normas ISO/IEC 27001:2022 e ISO 22301:2012.	En desarrollo de la acción de mejoramiento, el Grupo TIC elaboró el documento GSI-PL-002 "Plan de Continuidad del Negocio (BCP)", versión 1.0, el cual contempla el análisis de impacto al negocio (BIA), la identificación de procesos críticos, la matriz de riesgos y amenazas, las estrategias de continuidad, el Comité de Crisis, el plan de comunicaciones, los procedimientos de respuesta, el plan de pruebas y la metodología para su implementación y mantenimiento. Esta evidencia refleja el avance en las actividades orientadas a gestionar la aprobación formal del Plan de Continuidad del Negocio por parte de la Alta Dirección.
Se verificó que la entidad ha identificado, valorado y documentado los riesgos institucionales relacionados con la seguridad de la información. Durante la auditoría se validó el Mapa de Riesgos por Proceso publicado en la intranet para 2024, y se revisó la nueva matriz 2025, estructurada conforme al Modelo de Seguridad y Privacidad de la Información del Gobierno Digital. La matriz incluye controles aplicados, responsables asignados y evidencias de seguimiento, lo cual permite validar el cumplimiento de los controles A.5.4 y A.5.9 de la NTC ISO/IEC 27001:2022, así como los lineamientos del Decreto 620 de 2020 y la Resolución 02277 de 2025. La versión 2025 se encuentra en proceso de redacción y ajuste, por lo que aún no ha sido publicada oficialmente en los medios institucionales.	Finalizar, aprobar y publicar oficialmente el Mapa de Riesgos de Seguridad de la Información 2025, garantizando su actualización periódica, trazabilidad documental y alineación con el Sistema de Control Interno y el Modelo de Seguridad y Privacidad de la Información del Gobierno Digital.	La matriz de riesgos de seguridad de la información ha sido desarrollada en la nueva plantilla oficial sugerida por el MinTIC. Se encuentra en etapa de revisión previa a su aprobación y publicación formal.	La documentación aportada para esta acción de mejoramiento corresponde al Mapa de Riesgos de Seguridad de la Información 2025, elaborado en la plantilla oficial del MinTIC, así como a la publicación realizada en la intranet institucional. La evidencia revisada permitió corroborar que el documento se encuentra publicado en los medios institucionales y refleja el avance de las actividades orientadas a la actualización y divulgación del Mapa de Riesgos de Seguridad de la Información.
Se verificó que la entidad no cuenta con un documento formal del Modelo de Arquitectura	Formalizar el Modelo de Arquitectura Empresarial	Dado que CORPAMAG no cuenta actualmente con una arquitectura	Como evidencia del avance de la acción de mejoramiento, se aportó el documento

Descripción del hallazgo	Acción de mejora	Estado	Resultado del seguimiento
Empresarial (MAE) implementado conforme al Marco de Referencia de Arquitectura Empresarial (MRAE) del MinTIC. Sin embargo, se evidenció que se ha elaborado el Plan Estratégico de Tecnologías de la Información (PETI) 2024–2027, el cual incorpora fases metodológicas definidas en el MRAE (comprender, analizar, construir y presentar), así como dominios estratégicos como Gobierno, Información, Infraestructura, Seguridad y Apropiación. Este documento constituye un insumo técnico base para la construcción del MAE, pero no se evidenció su formalización, registro en el portal del MinTIC ni aprobación por parte de la alta dirección, lo cual limita el cumplimiento del marco normativo vigente.	(MAE) de CORPAMAG conforme al Marco de Referencia de Arquitectura Empresarial (MRAE) versión 3.0 del MinTIC, tomando como base el PETI 2024–2027, garantizando su aprobación institucional, registro en el portal del MinTIC y alineación con la Resolución 1978 de 2023.	empresarial implementada, el desarrollo de este ítem requiere la participación articulada de todas las áreas de la Corporación. Se tomará como insumo principal el PETI vigente y se adelantará el proceso de construcción del MAE conforme a los lineamientos del MRAE versión 3.0 del MinTIC y la Resolución 1978 de 2023.	técnico "Modelo de Arquitectura Empresarial (MAE)" de CORPAMAG, versión 1.0, elaborado conforme al Marco de Referencia de Arquitectura Empresarial (MRAE) v3.0 del MinTIC y tomando como base el PETI 2024–2027. El documento desarrolla el contexto institucional, los seis dominios del MRAE, el análisis de brechas, la hoja de ruta y las actividades previstas para su aprobación institucional y posterior registro ante el MinTIC. La evidencia presentada corresponde al desarrollo de la primera actividad del plan de mejoramiento; las actividades relacionadas con su aprobación mediante resolución y su registro en el portal del MinTIC continúan dentro del plazo establecido para su ejecución.
Se evidenció que la entidad realizó el autodiagnóstico de seguridad y privacidad de la información mediante la herramienta del Modelo MSPI entre el 17 de julio y el 31 de agosto de 2023, obteniendo un nivel de madurez crítico, con un promedio de efectividad de controles del 6% y un avance del ciclo PHVA también del 6%. El resultado fue incorporado como insumo en el PETI 2024–2027, donde se reconocen las debilidades identificadas y se proyectan metas progresivas de implementación del MSPI (40% en 2025, 70% en 2026 y 100% en 2027). Sin embargo, no se aporta evidencia documental sobre la aprobación formal del diagnóstico ni su presentación ante el Comité de Gestión y Desempeño Institucional, como lo exige el ítem. Esta ausencia limita la trazabilidad institucional y la validación del proceso conforme a los lineamientos del Modelo de Seguridad y Privacidad de la Información del Gobierno Digital.	Formalizar la aprobación del autodiagnóstico de seguridad y privacidad de la información realizado mediante el Modelo MSPI, documentando su validación y presentación ante el Comité de Gestión y Desempeño Institucional, en cumplimiento del Decreto 620 de 2020 y la Resolución 02277 de 202	https://nube.corpamag.gov.co/d/s/18F3qpkNETc1cPbFzZRrVxRPZMEJsQmw/ujEwF0EDF5DIqiHSkA5EkaTvEVD1cpdw-xLcAK3JcNw0	A la fecha del seguimiento no se evidencian avances en las actividades previstas; sin embargo, estas continúan dentro del plazo definido para su ejecución.
Se verificó que la entidad se encuentra en etapa de planeación preliminar para la adopción del modelo de IPv6 definido por el MinTIC. El cronograma institucional contempla cinco fases entre el cuarto trimestre de 2025 y el cuarto trimestre de 2026, incluyendo diagnóstico, diseño de red, políticas de seguridad, pruebas en ambiente controlado, migración progresiva y evaluación final. Sin embargo, no se aporta evidencia documental que permita verificar la aprobación formal del cronograma ni la adopción institucional del modelo, y no se evidencian avances técnicos, pruebas ni implementación de ninguna de las fases proyectadas. De acuerdo con la Resolución 1126 de 2021, el plazo para la implementación del protocolo IPv6 en entidades del orden nacional venció el 30 de	Formalizar y aprobar el cronograma institucional para la adopción del protocolo IPv6, y ejecutar las fases de diagnóstico, diseño, pruebas y migración conforme a la Resolución 1126 de 2021, garantizando la interoperabilidad, continuidad y cumplimiento normativo en la infraestructura tecnológica de CORPAMAG.	Se está ajustando el cronograma de adopción del protocolo IPv6, el cual incluirá las fases de diagnóstico, diseño, pruebas y migración, conforme a la Resolución 1126 de 2021.	La evidencia aportada para esta acción de mejoramiento corresponde al documento relacionado con la adopción del protocolo IPv6. Durante su revisión se observó que, aunque el soporte de ejecución reporta como completada la actividad correspondiente a la aprobación del cronograma institucional, no se aportó el documento que permitiera corroborar dicho avance. En consecuencia, la documentación revisada refleja el inicio de las actividades orientadas a la adopción del protocolo IPv6, sin que fuera posible verificar la aprobación formal del cronograma reportada por el auditado.

Descripción del hallazgo	Acción de mejora	Estado	Resultado del seguimiento
junio de 2022. A la fecha de corte de la auditoría, la entidad no cumple con dicho requerimiento, lo cual limita la trazabilidad institucional y el cumplimiento normativo en materia de transición tecnológica.			
Se constató que la entidad pública conjuntos de datos abiertos en su portal institucional y los ha registrado en el portal nacional www.datos.gov.co, en cumplimiento de la Política de Gobierno Digital y la Resolución 1519 de 2020. Los conjuntos definidos incluyen: - Índice de información clasificada y reservada - Registro de activos de información - Esquema de publicación de información - Monitoreo de la calidad del aire del departamento del Magdalena En el sitio web institucional, los cuatro conjuntos cuentan con enlaces activos y funcionales. En el portal nacional, todos están registrados y actualizados en estructura y metadatos. Sin embargo, el conjunto de calidad del aire, cuya frecuencia de actualización es mensual, presenta información consolidada hasta febrero de 2024, lo cual limita la vigencia del dato frente a su periodicidad declarada.	Actualizar el conjunto de datos abiertos de calidad del aire conforme a su frecuencia mensual declarada, garantizando la vigencia, trazabilidad y cumplimiento de la Resolución 1519 de 2020 y los lineamientos de la Política de Gobierno Digital.	El conjunto de datos abiertos de calidad del aire ha sido actualizado conforme a su frecuencia mensual declarada. El avance es verificable en línea en el portal correspondiente. https://www.datos.gov.co/Ambiente-y-Desarrollo-Sostenible/Monitoreo-Calidad-de-Aire-departamento-del-Magdale/dgnf-6h7v/about_data	Se corroboró en el portal nacional de datos abiertos que el conjunto de datos de monitoreo de calidad del aire fue actualizado hasta abril de 2026, evidenciando un avance frente a la situación identificada en la auditoría. No obstante, teniendo en cuenta que la frecuencia de actualización definida para este conjunto de datos es mensual y la acción de mejoramiento continúa en ejecución, su actualización periódica será verificada en los próximos seguimientos.
Se verificó que la entidad no ha documentado lecciones aprendidas en proyectos con componentes TI. La Oficina de Tecnologías de la Información manifiesta que se encuentra avanzando en la definición de una metodología para formalizar esta práctica, reconociéndola como fundamental para fortalecer la gestión del conocimiento institucional. Sin embargo, no se aporta evidencia que permita verificar los avances mencionados. Como única evidencia se remite una planilla en formato de matriz, sin registros diligenciados ni documentos que respalden su aplicación efectiva (informes de cierre, actas de socialización o consolidación de aprendizajes). Esta situación limita la trazabilidad del aprendizaje organizacional y la retroalimentación técnica en proyectos TIC.	Diseñar, formalizar e implementar una metodología institucional para documentar y socializar las lecciones aprendidas en proyectos con componentes TI, garantizando su aplicación y trazabilidad como parte de la gestión del conocimiento institucional.		A la fecha del seguimiento no se evidencian avances en las actividades previstas; sin embargo, estas continúan dentro del plazo definido para su ejecución.
La entidad no ha definido ni implementado estrategias para consolidar el conocimiento técnico del área TI. Aunque se señala que se está en etapa de análisis, no se aportaron evidencias que permitan verificar avances en la estructuración o aplicación de dichas estrategias, como planes formales, repositorios funcionales o cronogramas de capacitación, lo que impide validar su cumplimiento.	Definir e implementar estrategias institucionales para consolidar el conocimiento técnico del área TI, mediante la creación de planes de formación, repositorios documentales y mecanismos de intercambio de buenas prácticas, en coherencia con la Política de Gobierno Digital y los principios de mejora continua.	Se está diseñando el plan de formación del área de TI, el cual contemplará la creación de repositorios documentales y mecanismos de intercambio de buenas prácticas, en coherencia con la Política de Gobierno Digital.	A la fecha del seguimiento no se evidencian avances en las actividades previstas; sin embargo, estas continúan dentro del plazo definido para su ejecución.

Descripción del hallazgo	Acción de mejora	Estado	Resultado del seguimiento
Conforme a lo expresado por el equipo técnico, La entidad no dispone de un servidor conforme a las especificaciones técnicas del anexo 2 del Decreto 620 de 2020 para vincularse al servicio de interoperabilidad. Aunque se ha documentado un proceso técnico en etapa de planeación preliminar, no se evidencian elementos que permitan validar la implementación, como ficha técnica del servidor, acta de vinculación o pruebas de conexión exitosas.	Continuar con el proceso técnico para disponer de un servidor conforme a las especificaciones del anexo 2 del Decreto 620 de 2020, garantizando la vinculación efectiva al servicio de interoperabilidad y fortaleciendo la trazabilidad institucional en el intercambio de información.	Se está adelantando el estudio del proceso de interoperabilidad institucional, con especial atención a la integración con INVEMAR, como caso de uso prioritario para la vinculación efectiva al servicio de interoperabilidad.	A la fecha del seguimiento no se evidencian avances en las actividades previstas; sin embargo, estas continúan dentro del plazo definido para su ejecución.
La entidad no tiene implementado el uso de datos externos para apoyar decisiones misionales. Aunque se proyecta avanzar en la identificación de fuentes externas y en su integración institucional, no se evidencian mecanismos formales ni documentos que respalden su aplicación,	Formalizar e implementar el uso de datos externos como insumo para la toma de decisiones misionales, identificando fuentes confiables, estableciendo criterios de integración y garantizando su alineación con el Manual de Gobierno Digital y la Directiva Presidencial 003 de 2021.	https://nube.corpamag.gov.co/d/s/18F3sKSXC5EjRSSvfsq8vHQoj9Y9C7ll/KeMYLc3TzruYHQ_g4pXO4XUYZtg68q1C-jbjAmJhfNw0	La documentación aportada corresponde a un documento técnico en el que se identifican las fuentes externas de datos relevantes para apoyar la toma de decisiones institucionales. La evidencia revisada refleja el avance en la identificación y documentación de dichas fuentes.
Se verificó en el sitio web institucional que la entidad cuenta con 24 trámites ambientales digitalizados, inscritos en el Sistema Único de Información de Trámites (SUIT) y gestionados mediante integración con la plataforma VITAL del Ministerio de Ambiente.	Ajustar el menú del sitio web institucional para incluir un ítem visible denominado “Trámites y Servicios” dentro del apartado de Atención y Servicios a la Ciudadanía, facilitando el acceso y la comprensión de los trámites digitales por parte de los usuarios.	El ajuste ha sido implementado. El ítem «Trámites y Servicios» se encuentra visible en el apartado de Atención y Servicios a la Ciudadanía del sitio web institucional y es verificable en línea. https://corpamag.gov.co/	Se corroboró en el sitio web institucional la incorporación del acceso a los trámites ambientales dentro del menú "Atención y Servicios a la Ciudadanía", mediante el ítem "Oferta Institucional – Trámites Ambientales", el cual direcciona correctamente a los trámites disponibles para los usuarios. La evidencia revisada permite dar por cumplida la acción de mejoramiento propuesta..

Fuente: Elaboración propia OCI CON información suministrada Grupo TIC

9. Conclusiones

Como resultado del seguimiento efectuado, se evidenciaron avances en la implementación de las acciones formuladas por la entidad, particularmente en la actualización de documentos asociados a la seguridad y privacidad de la información, la elaboración de instrumentos técnicos del Modelo de Seguridad y Privacidad de la Información (MSPI), la formulación del Plan de Continuidad del Negocio, la actualización del mapa de riesgos y el desarrollo de iniciativas relacionadas con la Política de Gobierno Digital.

Asimismo, se observó que varias de las actividades definidas en el Plan de Mejoramiento Institucional presentan diferentes niveles de ejecución y continúan dentro de los plazos establecidos, permitiendo evidenciar progresos en la gestión de la seguridad de la información y en la adopción gradual de los requisitos establecidos en la Norma Técnica Colombiana NTC ISO/IEC 27001:2022.

No obstante, aún permanecen pendientes aspectos relacionados con la formalización de algunos documentos institucionales, la implementación de procedimientos para la gestión de proveedores, la adopción del protocolo IPv6, la consolidación de mecanismos de interoperabilidad y la solución definitiva de las condiciones físicas del cuarto de servidores, los cuales requerirán continuar avanzando en su implementación y serán objeto de los seguimientos que adelante la Oficina de Control Interno, de conformidad con las actividades programadas.

10. Recomendaciones

Continuar adelantando las acciones necesarias para la implementación y consolidación de las medidas definidas en el Plan de Mejoramiento Institucional, con el fin de fortalecer la gestión de la seguridad de la información y asegurar el cumplimiento de los requisitos establecidos en la Norma Técnica Colombiana NTC ISO/IEC 27001:2022 y de los lineamientos asociados a la Política de Gobierno Digital.

Para constancia se firma en Santa Marta D.T.C.H., a los siete (7) días del mes de julio de 2026.

LILIANA HIDALGO GARCÍA
Jefe Oficina de Control Interno

LUZ PIEDAD ECHAVARRÍA LÓPEZ
Contratista

Anexo: Seguimiento Plan de Mejoramiento.