Agencia Nacional de Minería

IMPLEMENTACION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MSPI

INFORME DE AUDITORIA INTERNA

WILMA ROCIO BEJARANO GAITAN
Jefe Control Interno

Equipo Auditor:

Diego Alexander Urazán Franco

Juan David Parga Moreno

Alcenides Martínez Arteaga

OFICINA DE CONTROL INTERNO

2026

ANM-OCI-033-2026

Tabla de contenido.

1. OBJETIVO

Evaluar el grado de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad, verificando su alineación con las actualizaciones de la normatividad asociada en el marco de la Política de Gobierno Digital.

2. OBJETIVOS ESPECIFICOS

- ✓ Validar el diligenciamiento del instrumento de autodiagnóstico MSPI, verificando la consistencia entre lo reportado por la entidad, las evidencias aportadas como soporte, las calificaciones asignadas y las brechas identificadas para cada uno de los controles.
- ✓ Validar la ejecución de las fases establecidas en el Modelo de Seguridad y Privacidad de la Información —diagnóstico, planificación, operación, evaluación del desempeño y mejoramiento continuo— y su nivel de avance en la entidad.

3. ALCANCE

El alcance comprendió la verificación de la gestión realizada para la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI en la entidad, cubriendo el periodo del 1 de enero al 31 de diciembre de 2025. Conforme a la facultad de ampliación prevista en el programa de trabajo, se incorporaron validaciones de documentos emitidos en la vigencia 2026.

4. MARCO NORMATIVO

- ✓ Resolución número 02277 del 2025 - Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.
- ✓ Resolución 746 de 2022 – MinTIC - Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución número 500 de 2021.
- ✓ Resolución 500 de 2021 – MinTIC - Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

5. METODOLOGIA

La auditoría a la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) se desarrolló aplicando técnicas de auditoría orientadas a la obtención de evidencia suficiente, competente y pertinente, conforme a los lineamientos de auditoría interna y control aplicables a las entidades públicas.

En una primera etapa, el equipo auditor formuló una solicitud inicial de información, la cual fue atendida y remitida por la Oficina de Tecnologías e Información (OTI) sin limitaciones para el desarrollo del ejercicio. Posteriormente, se llevó a cabo una sesión de contexto en la que la OTI y el Oficial de Seguridad de la Información expusieron el estado de implementación del Modelo en la entidad, lo cual permitió delimitar los aspectos objeto de verificación. Con base en lo anterior, se aplicaron las siguientes técnicas de auditoría:

- ✓ **Cotejo documental:** comparación y verificación de la información remitida por la OTI frente a la normatividad vigente, los lineamientos aplicables al Modelo, los instrumentos institucionales y los documentos de planeación y gestión de la entidad.
- ✓ **Validación en el sitio web institucional:** verificación de la publicación y disponibilidad de la información asociada al Modelo en los canales dispuestos por la entidad, contrastando lo publicado frente a los requisitos aplicables.
- ✓ **Verificación de cumplimiento:** comprobación del grado de cumplimiento de los requisitos legales, técnicos y procedimentales aplicables al Modelo, mediante la revisión de registros, evidencias y documentos soporte.
- ✓ **Análisis de información:** evaluación de la consistencia, pertinencia y suficiencia de la información suministrada por la entidad, con el fin de identificar fortalezas, oportunidades de mejora y aspectos susceptibles de fortalecimiento en la implementación del Modelo.

6. RESULTADOS

En el marco de la presente auditoría, el equipo auditor de la Oficina de Control Interno adelantó la evaluación al Modelo de Seguridad y Privacidad de la Información – MSPI, con el fin de establecer el estado de su implementación en la entidad y verificar la efectividad de la gestión realizada para su operación y mejora continua, así como medir el grado de cumplimiento frente a los requerimientos normativos y técnicos aplicables a las entidades públicas.

El ejercicio se orientó a determinar el nivel de madurez institucional del MSPI, revisando la aplicación práctica de lo definido en el Documento Maestro del Modelo de Seguridad y Privacidad de la Información versión 5, el cual se estructura en cinco fases:

1. Diagnóstico.
2. Planificación.
3. Operación.
4. Evaluación del desempeño.
5. Mejoramiento continuo.

Gráficamente el modelo se expresa como se presenta en la Imagen 1:

Imagen 1 Ciclo del Modelo de Seguridad y Privacidad de la Información – MSPI

Fuente: Documento Maestro del Modelo de Seguridad y Privacidad de la Información versión 5, MinTIC.

Con base en estas fases, los siguientes son los resultados obtenidos por el equipo auditor:

6.1. Diagnóstico:

El Documento Maestro define esta fase en los siguientes términos: "*La fase de diagnóstico permite a las entidades establecer el estado actual de la implementación de la seguridad y privacidad de la información, para tal fin se debe realizar un "Diagnóstico" utilizando el "instrumento de evaluación MSPI"; con el que se identifica de forma específica los controles implementados, se mide el nivel de madurez de la implementación del modelo de seguridad y privacidad de la información y se obtienen insumos fundamentales para la fase de planificación*."

Ante esto, y con base en validación realizada con la OTI, el instrumento para la vigencia 2026 presenta los siguientes datos, relacionados en la Imagen 2 y en la Imagen 3:

Imagen 2 Evaluación de efectividad de controles del MSPI por dominio

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	84	100	OPTIMIZADO
A.6	CONTROLES DE PERSONAS	90	100	OPTIMIZADO
A.7	CONTROLES FÍSICOS	89	100	OPTIMIZADO
A.8	CONTROLES TECNOLÓGICOS	79	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		86	100	OPTIMIZADO

Fuente: Matriz de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), diligenciada por la Oficina de Tecnologías de la Información (OTI) - 2026.

Imagen 3 Brecha de cumplimiento frente al Anexo A de la Norma NTC-ISO/IEC 27001:2022, por dominio de controles.

Fuente: Matriz de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), diligenciada por la Oficina de Tecnologías de la Información (OTI) - 2026.

De acuerdo con los resultados del instrumento de autodiagnóstico, la entidad presenta un nivel de madurez global "**Optimizado**", con una calificación promedio de 86 frente a una meta de cumplimiento de 100. Los controles organizacionales (84), de personas (90) y físicos (89) alcanzan igualmente el nivel "Optimizado", mientras que los controles tecnológicos (79) se ubican en nivel "Gestionado", constituyéndose en el dominio con mayor oportunidad de fortalecimiento.

Ahora bien, respecto al avance de cláusulas del modelo de operación (PHVA), fueron reportados los siguientes resultados, relacionados en la Imagen 4:

Imagen 4 Avance de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) por componente del ciclo PHVA y cláusula de la Norma NTC-ISO/IEC 27001:2022.

AÑO	COMPONENTE (PHVA)	CLAUSULAS	% de Avance Actual	% Avance Esperado
2025	Planificación	Contexto de la organización	10%	14%
		Liderazgo	12%	14%
		Planificación	8%	14%
		Soporte	13%	14%
	Implementación	Operación	15%	16%
	Evaluación de Desempeño	Evaluación del desempeño	12%	14%
	Mejora Continua	Mejora	14%	14%
TOTAL			84%	100%

Fuente: *Matriz de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), diligenciada por la Oficina de Tecnologías de la Información (OTI) - 2026.*

Al cierre de la vigencia 2025, el Modelo de Seguridad y Privacidad de la Información – MSPI presentó un avance global del **84**% frente a una meta esperada del 100%, evidenciando una gestión activa bajo el ciclo PHVA.

- En Planificación, las cláusulas de Contexto de la organización (10%), Liderazgo (12%), Planificación (8%) y Soporte (13%) se ubicaron por debajo de la meta del 14%, reflejando la necesidad de reforzar la documentación de estos procesos base.
- En Operación se alcanzó un 15% frente al 16% esperado.
- En Evaluación del Desempeño un 12% frente al 14%, mientras que
- Mejora Continua cumplió en su totalidad la meta con un 14%.

Conforme a lo anterior, la verificación se centró en el instrumento de evaluación MSPI diligenciado por la entidad, a partir del cual se contrastó lo reportado con las evidencias aportadas, las calificaciones asignadas y las brechas identificadas para cada control. Los resultados de esta revisión se presentan a continuación:

6.2. Levantamiento de información:

Resultados del levantamiento de información

Para la fase de diagnóstico, el instrumento de autodiagnóstico MSPI incorpora un levantamiento de información integrado por 42 ítems, orientados a identificar el estado actual de la entidad respecto a la implementación de la seguridad y privacidad de la información. A continuación, se detalla lo evidenciado por el equipo auditor en cada uno de los aspectos evaluados, según se relaciona en la Tabla 1:

Tabla 1 Elementos asociados a levantamiento de información para MSPI

NO.	Lista de información a solicitar	OBSERVACIONES OCI	NIVEL DE CUMPLIMIENTO
1	Tipo de entidad (Nacional, Territorial y categoría)	Se valida que la entidad corresponde al orden nacional.	CUMPLE
2	Misión	La redacción de la misión aportada en el instrumento indica "*liderar la transformación de la actividad minera en Colombia, administrando eficientemente los recursos minerales del Estado para impulsar el desarrollo sostenible, la competitividad del sector y la contribución económica, asegurando transparencia, responsabilidad social y ambiental en todo el proceso minero".* Esta no corresponde a la descrita en la página web institucional, la cual indica: "*Misión: Administrar los recursos mineros, planear y promover su aprovechamiento en el marco del interés general, el respeto de los Derechos Humanos y los determinantes ambientales, garantizando la responsabilidad social, la coordinación del Estado central y las entidades territoriales para generar desarrollo económico, equidad y paz."* Por lo indicado, se recomienda actualizar la información del instrumento.	NO CUMPLE
3	Análisis de contexto: La entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el MSPI.	El análisis presentado es general y descriptivo; se recomienda fortalecer la identificación de factores internos y externos asociados específicamente a riesgos de seguridad y privacidad de la información.	CUMPLE
4	Mapa de Procesos	El mapa de procesos se encuentra disponible en línea.	CUMPLE

NO.	Lista de información a solicitar	OBSERVACIONES OCI	NIVEL DE CUMPLIMIENTO
5	Organigrama de la entidad, detallando el área de seguridad de la información o quien haga sus veces	El organigrama aportado no permite identificar claramente la subordinación del área o rol responsable de la seguridad de la información.	PARCIAL
6	Políticas de seguridad de la información formalizada y firmada	Se verifica que la entidad cuenta con la política general formalizada en el Manual de Políticas de Seguridad de la Información APO4-M-002 V2, vigente desde el 10 de diciembre de 2024, aprobado por la Presidencia y publicado en el sistema integrado de gestión.	CUMPLE
7	Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.	La evidencia se soporta en el numeral 4.4 del manual de políticas, que desarrolla los roles frente al SGSI (Alta Dirección, Comité, OTI, Oficial de Seguridad y propietario del activo). Sin embargo, se referencia únicamente el numeral 4.4.1, omitiendo la asignación detallada de responsabilidades de los numerales 4.4.2 y 4.4.3. Se recomienda precisar las referencias y verificar la actualización anual de la matriz de roles exigida por el numeral 4.17.8.	CUMPLE
8	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección	No se evidencia documentación objetiva que certifique la aplicación y el resultado de la autoevaluación periódica del MSPI para la vigencia evaluada.	NO CUMPLE
9	Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado, aprobado y aceptado por la alta dirección	No se evidencia documentación o soporte técnico del diligenciamiento y los resultados consolidados de la encuesta de diagnóstico sectorial.	NO CUMPLE
10	Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la alta dirección	No se evidencia documentación formal que valide el proceso de estratificación de la entidad aceptado ante los entes correspondientes.	NO CUMPLE
11	Objetivo, alcance y límites del MSPI (Modelo de Seguridad y Privacidad de la Información)	Es importante notar que el documento utiliza principalmente la denominación Sistema de Gestión de la Seguridad de la Información (SGSI) para referirse a lo que comúnmente se conoce en el marco de Gobierno Digital como MSPI	CUMPLE

NO.	Lista de información a solicitar	OBSERVACIONES OCI	NIVEL DE CUMPLIMIENTO
12	Procedimientos de control documental del MSPI	Se evidencian los procedimientos de control documental integrados en el sistema de gestión de calidad, aplicando las reglas de retención y codificación vigentes.	CUMPLE
13	Metodología de Gestión de riesgos	Se evidencia que la metodología de gestión de riesgo se encuentra aprobada y formalizada institucionalmente mediante la guía de administración de riesgos de la entidad.	CUMPLE
14	Riesgos identificados y valorados de acuerdo a la metodología	Se observan mapas de riesgo publicados y actualizados periódicamente en los canales oficiales de la entidad de acuerdo con la política de riesgos.	CUMPLE
15	Planes de tratamiento de los riesgos	Se evidencia que la entidad cuenta con el plan de tratamiento de riesgos.	CUMPLE
16	Formatos de acuerdos contractuales con empleados y contratistas para establecer responsabilidades de las partes en seguridad de la información	El Acuerdo de Confidencialidad cumple con los requisitos generales para la protección de la información de la Agencia Nacional de Minería (ANM), definiendo de manera clara las obligaciones del contratista, el manejo de la información confidencial, las medidas de seguridad, las excepciones y las consecuencias por incumplimiento.	CUMPLE
17	Procedimiento de verificación de antecedentes para candidatos a un empleo en la entidad	En el seguimiento realizado se evidenció que el documento asociado en Isolucion corresponde al procedimiento CA-P-001, el cual no guarda relación con el control evaluado. En este sentido, se recomienda vincular el procedimiento correspondiente que soporte la verificación de antecedentes para candidatos a un empleo en la entidad. De otra parte, se observó que la lista de chequeo se encuentra estructurada de forma clara y organizada, permitiendo verificar el cumplimiento de los requisitos precontractuales, contractuales y de ejecución.	CUMPLE
18	Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado y aprobado por la alta Dirección, con sus respectivos soportes.	Se evidencia la existencia del Plan de Comunicación, Sensibilización y Capacitación en Seguridad de la Información, el cual se encuentra revisado y aprobado por la Alta Dirección.	CUMPLE

NO.	Lista de información a solicitar	OBSERVACIONES OCI	NIVEL DE CUMPLIMIENTO
19	Documento que haga claridad sobre el proceso disciplinario en caso de incumplimiento de las políticas de seguridad de la información	Se evidenció que el Manual de Políticas de Seguridad y Privacidad de la Información APO4-M-002 V2 contempla en su numeral 4.10.6 «Procesos Disciplinarios» el tratamiento aplicable frente al incumplimiento de los lineamientos establecidos en dicho documento, señalando que la entidad sigue los parámetros de los procedimientos internos definidos para el efecto.	CUMPLE
20	Inventario de activos de información clasificados, de la entidad, revisado y aprobado por la alta dirección	Se verificó el Registro de Activos de Información publicado en el portal web institucional, evidenciándose la disponibilidad de los registros correspondientes a las vigencias 2014 a 2025. Como parte de la prueba de auditoría, se confirmó la publicación y disponibilidad de la totalidad de los registros para cada una de las vigencias evaluadas, incluyendo el Registro de Activos de Información 2025, en concordancia con lo reportado en el instrumento de verificación.	CUMPLE
21	Inventario de áreas de procesamiento de información y telecomunicaciones	No se evidencia documentación formal que valide el proceso.	NO CUMPLE
22	Diagrama de red de alto nivel o arquitectura de TI	Según lo informado en el instrumento, el documento asociado está publicado en SECOP II del documento "3. ANEXO ESPECIFICACIONES Y REQUERIMIENTOS TÉCNICOS MÍNIMOS PRIORIZADOS V3", el cual contiene las especificaciones técnicas del proceso. No obstante, no se evidenció la existencia ni la publicación del diagrama de red de alto nivel, documento que constituye un insumo relevante para la comprensión de la arquitectura y la infraestructura tecnológica objeto del proceso. Se recomienda elaborar e implementar un diagrama de red de alto nivel que documente la arquitectura general de la solución, identificando los principales componentes, interconexiones y flujos de comunicación.	NO CUMPLE
23	Inclusión de la seguridad de la información en la gestión de proyectos	Se evidenció que la entidad cuenta con un Procedimiento de Gestión de Proyectos documentado en la plataforma Isolucion, el cual incorpora consideraciones de seguridad de la información durante el ciclo de vida de los proyectos. Se recomienda verificar que los proyectos de tecnologías de la información apliquen este procedimiento y que se conserven evidencias de la evaluación y tratamiento de los riesgos de seguridad de la información en cada proyecto.	CUMPLE
24	Inventario de partes externas o terceros a los que se transfiere información de la entidad	En el instrumento MSPI no se reporta información acerca de este aspecto.	NO CUMPLE

NO.	Lista de información a solicitar	OBSERVACIONES OCI	NIVEL DE CUMPLIMIENTO
25	Formato de acuerdo de transferencia de información	Se evidenció que la entidad cuenta con el Procedimiento de Intercambio de Información, documentado en la plataforma Isolucion, el cual establece los lineamientos para la transferencia de información entre las partes involucradas.	CUMPLE
26	Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden	Se evidenció el archivo PROVEEDORES_TI_ANM remitido por la OTI, en el cual se relacionan los contratos de servicios de tecnología con su objeto, proveedor y fecha de terminación, acreditando el inventario de proveedores. Se recomienda depurar los registros duplicados e incorporar el nivel de acceso de cada proveedor a los activos de información.	CUMPLE
27	Reporte de eventos e incidentes de seguridad de la información de los últimos 12 meses.	Se evidenció que la entidad cuenta con un Procedimiento para la Gestión de Incidentes de Seguridad de la Información y con el registro de eventos e incidentes gestionados a través de la herramienta de mesa de ayuda CAST, considerada información clasificada.	CUMPLE
28	Plan de continuidad de la Entidad aprobado	La entidad dispone de un Plan de Recuperación ante Desastres (DRP) para los sistemas críticos y de una Consultoría de Continuidad del Negocio, documentos disponibles en la plataforma Isolucion.	CUMPLE
29	Inventario de obligaciones legales, estatutarias, reglamentarias, normativas relacionadas con seguridad de la información	Se validó el ítem en el portal institucional (anm.gov.co/normograma-de-la-agencia-nacional-de-mineria). La entidad cuenta con el Normograma consolidado y publicado (vigente al Primer Semestre 2026), que incorpora disposiciones de seguridad de la información como la Ley 1712 de 2014, la Ley 1581 de 2012, la Ley 1273 de 2009, la Resolución 500 de 2021 del MinTIC y el Decreto 767 de 2022. Al verificar el inventario completo se observó que no incorpora la norma ISO/IEC 27001 ni la Ley 603 de 2000. Por lo anterior, el levantamiento para este ítem se cumple de manera parcial. Se recomienda incorporar dichas disposiciones al Normograma.	PARCIAL
30	Listado de auditorías relacionadas con seguridad de la información realizadas en la entidad	Se evidenció que el listado del programa de auditorías correspondiente al período 2018–2025 contempla únicamente auditorías relacionadas con la Administración de Tecnologías de la Información. No se identificaron auditorías específicas orientadas a evaluar la gestión de la seguridad de la información, lo que limita la cobertura de aseguramiento sobre los riesgos asociados a la confidencialidad, integridad y disponibilidad de la información institucional.	CUMPLE

NO.	Lista de información a solicitar	OBSERVACIONES OCI	NIVEL DE CUMPLIMIENTO
31	Procedimientos, manuales, guías, directrices, lineamientos, estándares, instructivos relacionados con seguridad de la información, el modelo de seguridad y privacidad de la información de MinTic y Gobierno Digital	Se evidenció que la entidad cuenta con procedimientos, manuales y políticas, entre ellos el Procedimiento de Gestión de Riesgos, el Procedimiento de Gestión de Cambios, el Manual de Políticas de Seguridad de la Información, la Resolución 104 del 2 de marzo de 2018 y la Política de Tratamiento de Datos Personales y Seguridad de la Información, los cuales se encuentran alineados con el Modelo de Seguridad y Privacidad de la Información (MSPI) y la estrategia de Gobierno Digital. Asimismo, se identificó que los procedimientos de Gestión de Activos de Información y Gestión de Incidentes se encuentran en proceso de revisión, caracterización y publicación.	PARCIAL
32	Indicadores y métricas de seguridad de la información definidos.	Se evidenció que el Plan de Seguridad y Privacidad de la Información contempla indicadores para el seguimiento del desempeño del SGSI, entre ellos: Evolución de la Madurez del SGSI, Promedio de Evaluación de Controles, Cumplimiento de los Dominios de Seguridad de la Información (A.5–A.18), Estado de los Riesgos de Ciberseguridad, Nivel de Aseguramiento de la Plataforma Microsoft 365 y Gestión de Vulnerabilidades Técnicas.	CUMPLE
33	Declaración de aplicabilidad	La entidad dispone de la Declaración de Aplicabilidad (SoA) correspondiente a la vigencia 2025, documento clasificado y administrado por el proceso de Seguridad de la Información.	CUMPLE
34	Aceptación de los riesgos residuales por parte de los dueños de los riesgos	Se evidenció que la entidad cuenta con un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025, en el cual se documentan los riesgos identificados, las acciones de tratamiento y el nivel de riesgo residual.	CUMPLE
	Lista de información para aquellas entidades que hayan avanzado en la fase de IMPLEMENTACIÓN		
35	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	No se relaciona información de este aspecto dentro del instrumento MSPI.	NO CUMPLE
36	Avance en la ejecución del plan de tratamiento de riesgos	La información es administrada como clasificada por el proceso de Seguridad de la Información y constituye un mecanismo para monitorear el cumplimiento de las acciones y el progreso del plan.	CUMPLE

NO.	Lista de información a solicitar	OBSERVACIONES OCI	NIVEL DE CUMPLIMIENTO
37	Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.	Se evidenció que la entidad dispone de indicadores de gestión asociados al Modelo de Seguridad y Privacidad de la Información (MSPI), documentados en la Matriz SOA 2025. Estos indicadores constituyen un mecanismo para medir el desempeño y el nivel de implementación de los controles del SGSI.	CUMPLE
	Lista de información para aquellas entidades que hayan avanzado en la fase de EVALUACIÓN DE DESEMPEÑO		
38	Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.	No se relaciona información de este aspecto dentro del instrumento MSPI.	NO CUMPLE
39	Documento con el plan de auditorías internas y resultados, de acuerdo a lo establecido en el plan de auditorías, revisado y aprobado por la alta Dirección.	Se evidenció que el listado del programa de auditorías correspondiente al período 2018–2025 contempla únicamente auditorías relacionadas con la Administración de Tecnologías de la Información. No se identificaron auditorías específicas orientadas a evaluar la gestión de la seguridad de la información, lo que limita la cobertura de aseguramiento sobre los riesgos asociados a la confidencialidad, integridad y disponibilidad de la información institucional.	CUMPLE
40	Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección.	No se relaciona información de este aspecto dentro del instrumento MSPI.	NO CUMPLE
	Lista de información para aquellas entidades que hayan avanzado en la fase de MEJORA CONTINUA		
41	Documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección.	No se evidencia documentación formal reportada dentro del instrumento que valide el aspecto.	NO CUMPLE

NO.	Lista de información a solicitar	OBSERVACIONES OCI	NIVEL DE CUMPLIMIENTO
42	Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta dirección y verifique como se asegura que los hallazgos, brechas, debilidades y oportunidades de mejora se subsanen, para asegurar la mejora continua.	La Oficina de Control Interno ha venido dando continuidad a la evaluación del Modelo de Seguridad y Privacidad de la Información (MSPI), mediante la ejecución de auditorías en la vigencia 2025 y en el nuevo Plan Anual de Auditoría que se está ejecutando a la fecha del año 2026. Estas acciones demuestran la inclusión permanente del modelo dentro del ejercicio de control interno, contribuyendo al seguimiento del cumplimiento, a la identificación de oportunidades de mejora y al fortalecimiento del sistema de gestión de seguridad y privacidad de la información de la entidad.	CUMPLE

Fuente: Matriz de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), diligenciada por la Oficina de Tecnologías de la Información (OTI) - 2026.

Del ejercicio de verificación se establece que la entidad cuenta con una base documental que sustenta el Sistema de Gestión de Seguridad de la Información, soportada en su política general, los procedimientos de gestión documental, la metodología de riesgos y los controles asociados.

No obstante, la revisión permitió constatar que aún faltan algunos documentos para consolidar dicha base, entre ellos:

- El marco misional actualizado,
- Los resultados de la autoevaluación del modelo,
- La estratificación institucional y
- Los inventarios de áreas de procesamiento y de terceros a los que se transfiere información, así como
- Los soportes de planificación operacional, seguimiento y medición aprobados por la alta dirección.

Contar con estos insumos es determinante, en la medida en que constituyen la base sobre la cual se desarrollan las etapas posteriores del modelo; su incorporación permitirá que la entidad avance de manera sólida en la operación, evaluación y mejora del sistema.

Con base en lo indicado se presenta la siguiente oportunidad de mejora:

Oportunidad de Mejora No. 1: Levantamiento de información incompleto para la fase de Diagnóstico del MSPI.

El instrumento de autodiagnóstico incorpora un levantamiento de 42 ítems como insumo de la fase de Diagnóstico, del cual no fue posible acreditar la totalidad de los elementos durante el ejercicio auditor.

No se aportaron el marco misional actualizado, los resultados de la autoevaluación del modelo, la estratificación de la entidad, los inventarios de áreas de procesamiento y de terceros a los que se transfiere información, ni los soportes de planificación operacional, seguimiento y medición aprobados por la alta dirección.

Al constituir esta fase la línea base sobre la cual se estructuran la planificación, la operación, la evaluación del desempeño y el mejoramiento continuo, su levantamiento parcial impide dimensionar el estado real de la seguridad y privacidad de la información, deja por fuera del alcance del sistema actores y activos que lo condicionan, particularmente los terceros a los que se transfiere información, y expone a la entidad a que las fases posteriores se desarrollen sobre supuestos no verificados.

Recomendación:

Se sugiere al responsable de la implementación del MSPI completar y consolidar los 42 ítems del levantamiento de información, asegurando que cada numeral cuente con evidencia actualizada, verificable y aprobada por la instancia competente, con prioridad en la estratificación institucional y en los inventarios de áreas de procesamiento y de terceros, de manera que estos insumos sirvan de línea base para la revalidación del diagnóstico en la siguiente vigencia.

Por otra parte, a continuación, se presenta el resultado del seguimiento de los controles de seguridad y privacidad de la información utilizando el instrumento MSPI, con el fin de medir el nivel de madurez del modelo y obtener insumos para planificación y mejora continua.

La evaluación se organiza en cuatro dominios según NTC-ISO/IEC 27001:2022 Anexo A: organizacionales, personas, físicos y tecnológicos.

La OCI presenta los resultados por cada dominio, principalmente con lo registrado en el instrumento MSPI el cual ha sido gestionado por la OTI encargados de la implementación del modelo así:

6.3. Dominio controles organizacionales:

En la Tabla 2 se relacionan las observaciones de la Oficina de Control Interno sobre los controles organizacionales del Anexo A.

Tabla 2 Seguimiento a la efectividad de los controles organizacionales – Observaciones de la Oficina de Control Interno.

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
AD.1.1	A 5.1	Políticas de seguridad de la información	100	En el seguimiento al control de Políticas de seguridad de la información, se verifica que la entidad cuenta con la política general formalizada en el Manual de Políticas de Seguridad de la Información APO4-M-002 V2, vigente desde el 10 de diciembre de 2024, aprobado por la Presidencia y publicado en el sistema integrado de gestión, lo cual sustenta la calificación de 100 puntos otorgada. No obstante, se observa que el instrumento refiere el documento como "anexo 07", denominación que no corresponde al código y versión vigentes del manual. Se recomienda ajustar la referencia documental del instrumento y verificar que la revisión periódica de la política se realice conforme al numeral 4.3 del manual.
AD.1.2	A 5.2	Roles y responsabilidades de seguridad de la información	100	Para este control, la evidencia se soporta en el numeral 4.4 del manual de políticas, que desarrolla los roles frente al SGSI (Sistema de Gestión de Seguridad de la Información), alta Dirección, Comité Institucional de Gestión y Desempeño, OTI, Oficial de Seguridad y propietario del activo. Al contrastar lo declarado con el manual, se observa que el instrumento referencia únicamente el numeral 4.4.1, cuando la asignación detallada de responsabilidades por rol se encuentra en los numerales 4.4.2 y 4.4.3, los cuales no fueron referenciados. Si bien la calificación de 100 puntos resulta razonable, se recomienda precisar la referencia y verificar la matriz de roles y responsabilidades cuya actualización anual exige el numeral 4.17.8 del manual. De manera complementaria, se observa que el numeral 7.2.3 del documento maestro Guía de Implementación del MSPI exige que el responsable del modelo dependa de un área estratégica distinta a la de Tecnología y se designe mediante acto administrativo, con articulación al Comité Institucional de

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
				Gestión y Desempeño y al Comité de Control Interno. Al respecto, se identifica que la figura de Oficial de Seguridad de la Información se ejerce actualmente dentro de la Oficina de Tecnología e Información, situación que no resulta coherente con lo dispuesto en el documento maestro. Se recomienda a la entidad validar lo indicado en el documento maestro frente a este aspecto.
AD.1.3	A 5.3	Segregación de funciones	80	El equipo auditor respecto al control de Segregación de funciones, identifica que el campo de evidencia del instrumento se limita a una referencia genérica al procedimiento de control de acceso, sin sustentar de manera integral los aspectos que la prueba relaciona. Al contrastar lo declarado con el manual de políticas, este sí desarrolla el control en los numerales 4.4.4 y 4.17.8, que exigen la independencia mínima entre la administración de red, sistemas operativos, bases de datos, desarrollo, gestión de cambios y seguridad informática, lineamientos que no fueron referenciados en el instrumento. Adicionalmente, el Informe de Seguimiento de Vulnerabilidades del 4to trimestre de 2025 advierte un riesgo de segregación de funciones derivado de la concentración de labores en el equipo de infraestructura, situación relevante para este control. Se observa también que el campo de brecha no fue diligenciado, por lo que se recomienda documentar la matriz de segregación de funciones y precisar los aspectos pendientes por cumplir.
AD.1.4	A 5.4	Responsabilidades de la dirección	100	Para el control de Responsabilidades de la dirección, la evidencia se soporta en el numeral 4.4.3 literales a y b del manual, relativo a las responsabilidades de la alta Dirección y del Comité Institucional de Gestión y Desempeño en la aprobación, revisión y provisión de recursos del SGSI (Sistema de Gestión de Seguridad de la Información). Al verificar la referencia, se observa que el instrumento cita el numeral 4.4.1, que corresponde al deber general de cumplimiento y no a las responsabilidades de la dirección. Si bien la calificación de 100 puntos resulta consistente, se recomienda corregir la referencia y aportar como evidencia objetiva las actas del Comité Institucional de Gestión y Desempeño en las que conste la aprobación y el seguimiento del SGSI.

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
AD.1.5	A 5.5	Contacto con las autoridades	80	Se evidencia que la entidad definió en el numeral 4.4.5 del Manual de Políticas de Seguridad de la Información la directriz de contacto con las autoridades, disponiendo que la Agencia mantenga contacto actualizado con organismos de control y fuerzas del orden a través de los jefes de oficina y vicepresidentes. No obstante, ese mismo numeral asigna a la Oficina de Control Interno la definición, actualización y publicación del listado de autoridades y el contacto con las mismas, función operativa que no corresponde a su naturaleza de línea de aseguramiento independiente, encargada de evaluar el SGSI y no de ejecutarlo. Por ello se recomienda reasignar esta responsabilidad, dejando en la Oficina de Control Interno solo la evaluación independiente del control, de acuerdo a lo indicado en el Anexo A 5.5 de la NTC-ISO/IEC 27001:2022.
AD.1.6	A 5.6	Contacto con grupos de interés especial	80	Se identifica que la evidencia cita el documento de comunicación de crisis, sin acreditar la pertenencia o suscripción a foros y asociaciones de seguridad. El numeral 4.4.6 del manual asigna a la OTI el contacto con grupos de interés para recibir alertas de vulnerabilidades día cero y avisos de ciberataques. Se observa que el campo de brecha no fue diligenciado, por lo que se recomienda reportar las actividades pendientes para que la calificación llegue a 100.
AD.1.7	A 5.7	Inteligencia de amenazas	60	El equipo auditor valida respecto a este control estimado que la inteligencia de amenazas se realiza a través del SOC, Security Operations Center (Centro de Operaciones de Seguridad), sin acreditar los atributos que la prueba exige. Al contrastar lo declarado con el manual de políticas, se observa que este no desarrolla de manera específica este control, en la NTC-ISO/IEC 27001:2022. Pese a ello, se otorgó una calificación de 60 puntos sin que el campo de brecha precise los aspectos pendientes. Se recomienda revalidar la calificación y fortalecer los entregables asociados a este control.

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
AD.1.8	A 5.8	Seguridad de la información en la gestión de proyectos	100	En el seguimiento al control de Seguridad de la información en la gestión de proyectos, la evidencia se soporta en el numeral 4.5 del manual y en el instructivo de gestión de riesgos EST1-P-003-I-002, así como en el plan de la oficina PMO (Project Management Office) y en la matriz de riesgos contractuales APO1-P-001-F-030, lo cual sustenta la calificación de 100 puntos. Se observa que el instrumento cita el procedimiento de gestión de proyectos con el código APO4-P-003, cuya vigencia debe verificarse frente a la recodificación documental del sistema integrado de gestión adelantada en noviembre de 2025. Se recomienda confirmar la vigencia del código y aportar un registro de valoración de riesgos de seguridad aplicada a un proyecto reciente como evidencia de operación efectiva.
AD.1.9	A 5.9	Inventario de información y otros activos asociados	80	Se válida para este control que la evidencia aportada por la OTI demuestra la identificación y clasificación de los activos de información, de conformidad con los procedimientos establecidos por la entidad y adicional que se dispone de una CMDB (Configuration Management Database) que mantiene el inventario de los activos informáticos de hardware y software. Lo anterior se respalda adicionalmente en los entregables aportados: el Inventario de Activos de Información en formato MSPI (942 registros), el Registro de Activos de Información 2025 (596 registros) y el Índice de Información Clasificada y Reservada 2025 (233 registros), en concordancia con el numeral 4.11 del manual de políticas de seguridad de la información. Se recomienda incorporar como evidencia verificable un soporte asociado a lo descrito y diligenciar el campo brecha con el fin de tener claridad sobre los aspectos que harían falta para el total cumplimiento del control.
AD.1.10	A 5.10	Uso aceptable de la información y otros activos asociados	80	El equipo auditor identifica una inconsistencia en la referencia documental, toda vez que el instrumento cita el numeral 4.8.2, mientras que el uso aceptable de los activos se desarrolla en el numeral 4.11.1 del manual de políticas vigente (V2). Se observa además que el campo de brecha no fue diligenciado pese a la calificación de 80 puntos. Se recomienda corregir la referencia al numeral 4.11.1 y precisar los aspectos pendientes para alcanzar el cumplimiento total del control.

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
AD.1.11	A 5.11	Devolución de Activos	80	De acuerdo con lo validado por el equipo auditor, para este control, la evidencia se soporta en el sistema de paz y salvo y en los formatos de entrega de cargo (APO1-P-001-F-036, APO5-P-001-F-004 y APO5-P-001-F-003), en concordancia con el numeral 4.10.5 del manual. La calificación de 80 puntos resulta razonable; no obstante, se observa que el campo de brecha no fue diligenciado, con esto, no se puede tener claridad de cuáles serían las actividades o evidencias pendientes para legar a un cumplimiento de 100. Se recomienda relacionar los aspectos pendientes y aportar una muestra de paz y salvos suscritos como evidencia de operación del control.
AD.1.12	A 5.12	Clasificación de la información	80	En el seguimiento al control de Clasificación de la información, la evidencia del instrumento indica que la ANM realiza la clasificación de la información en todas sus áreas considerando la Ley 1581 de 2012 y la Ley 1712 de 2014, y que este lineamiento se establece en el procedimiento de gestión de activos de información de la ANM. Dicha clasificación se encuentra desarrollada en el numeral 4.11.4 del manual de políticas y se respalda en el documento titulado: Inventario Activos inf -ANM 2025-FORMATO MSPI, que incorpora la clasificación por confidencialidad, integridad y disponibilidad de cada activo y en el Índice de Información Clasificada y Reservada 2025 (233 registros). El procedimiento de gestión de activos de información se identifica con el código APO4-P-009. Se recomienda referenciar los entregables citados y diligenciar el campo de brecha.
AD.1.13	A 5.13	Etiquetado de la información	80	Para el tema de etiquetado de la información, la evidencia cita el Procedimiento de Gestión de Activos de Información, en línea con el numeral 4.11.2 literal d del manual. Se identifica que la evidencia acredita el lineamiento documental. En la operación diaria de la entidad se observan mecanismos que materializan el etiquetado en medios en que circula la información; por ejemplo, al remitir un correo electrónico el sistema solicita al usuario la clasificación correspondiente para proceder a registrar el etiquetado sobre la información transmitida, lo cual refleja la aplicación práctica del control más allá del plano documental. No obstante, la evidencia aportada no permite verificar que el etiquetado se aplique de manera consistente sobre la totalidad de los activos clasificados en el Inventario MSPI. Se observa además que el campo de brecha no fue

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
				diligenciado, por lo que se recomienda aportar evidencia del etiquetado aplicado sobre dichos activos y precisar en el instrumento los aspectos pendientes.
AD.1.14	A 5.14	Transferencia de información	100	En el seguimiento al control de Transferencia de información, la evidencia se soporta en el numeral 4.28.2 del manual y en el Procedimiento de Consulta y/o Intercambio de Información, citado con el código APO4-P-016, lo cual sustenta la calificación de 100 puntos. Se observa que dicho código debe verificarse frente a la recodificación del sistema integrado de gestión. Se recomienda confirmar la vigencia del código y aportar un registro de transferencia formal como evidencia de operación del control.
AD.1.15	A 5.15	Control de acceso	80	Respecto a control de Control de acceso, se identifica que este se soporta en el numeral 4.17 del manual, que desarrolla integralmente los principios de acceso a redes, la solicitud, suspensión, revisión e identificación de usuarios. Ahora bien, respecto a lo descrito en el instrumento por parte de la OTI, se identifica una posible inconsistencia de codificación, toda vez que el instrumento cita el procedimiento de control de acceso con el código APO4-P-007-001, mientras que en el manual el código APO4-P-007 se asocia a la gestión de incidentes (numeral 4.31). Se observa que el campo de brecha no fue diligenciado, por lo que se recomienda verificar y corregir el código del procedimiento y relacionar los aspectos pendientes.
AD.1.16	A 5.16	Gestión de la identidad	80	En el seguimiento al control de Gestión de la identidad, la evidencia se centra en la grabación de sesiones de cuentas privilegiadas mediante la plataforma CyberArk, asociada a los numerales 4.17.6 y 4.18.7 literal c del manual, según lo validado por el equipo auditor. Ante lo descrito y con base en la calificación otorgada, se recomienda complementar la evidencia y precisar los aspectos pendientes.
AD.1.17	A 5.17	Información de autenticación	80	Para el control de Información de autenticación, la evidencia describe la entrega de credenciales con cambio obligatorio en el primer ingreso, en concordancia con los numerales 4.17.7 y 4.18.1 literal f del manual. La calificación de 80 puntos resulta razonable en cuanto al lineamiento documental; no obstante, las pruebas de seguridad lógica aplicadas sobre el sistema ANNA Minería evidenciaron aspectos relacionados con los usuarios. En efecto, se identificaron cuentas genéricas activas,

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
				así como cuentas activas pertenecientes a personal retirado de la entidad, situaciones que reflejan deficiencias en la depuración de los accesos. Se observa además que el campo de brecha no fue diligenciado. Por lo anterior, se recomienda aportar evidencia de la parametrización de la política de contraseñas en los sistemas, en cuanto a longitud, vigencia e historial, adelantar la depuración de las cuentas genéricas y de personal retirado identificadas en ANNA Minería, y relacionar en el instrumento los aspectos pendientes.
AD.1.18	A 5.18	Derechos de acceso	100	En el seguimiento al control de Derechos de acceso, la evidencia se soporta en el procedimiento de control de acceso y en los numerales 4.17.3 a 4.17.5 del manual, relativos a la concesión, revisión y suspensión de accesos, lo cual sustenta la calificación de 100 puntos. Se recomienda aportar como evidencia de operación una muestra de las revisiones periódicas de derechos de acceso previstas en el numeral 4.17.5 del manual.
AD.1.19	A 5.19	Seguridad de la información en las relaciones con proveedores	80	En el seguimiento al control de Derechos de acceso, la evidencia se soporta en el procedimiento de control de acceso y en los numerales 4.17.3 a 4.17.5 del manual, relativos a la concesión, revisión y suspensión de accesos. Si bien el marco documental respalda la calificación de 100 puntos, las pruebas de seguridad lógica aplicadas sobre el sistema ANNA Minería evidenciaron cuentas activas de personal retirado y de contratistas cuya vinculación había finalizado, así como cuentas genéricas, situaciones que revelan que la revisión y suspensión oportuna de accesos prevista en el numeral 4.17.5. Por lo anterior, la calificación de 100 puntos no refleja la operación real del control. Se recomienda adelantar barridos periódicos de usuarios en los diferentes sistemas de información de la entidad, con el fin de depurar los accesos y establecer el valor real de la calificación, y aportar como evidencia de operación una muestra de las revisiones periódicas de derechos de acceso previstas en el numeral 4.17.5 del manual.
AD.1.20	A 5.20	Abordar la seguridad de la información en los	80	Validando el control de Abordar la seguridad de la información en los acuerdos con proveedores, la evidencia del instrumento señala que los proyectos cuentan con el compromiso de confidencialidad y aceptación de las políticas de seguridad de

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
		acuerdos con proveedores		la ANM. De igual manera en el manual de políticas de seguridad de la información, este control se desarrolla en el numeral 4.30.2 del manual, cuyo literal b) fija las cláusulas mínimas de los acuerdos con proveedores (confidencialidad, cumplimiento de políticas, reporte de eventos, etiquetado y seguimiento de servicios), según lo validado por el equipo auditor. Adicionalmente, se identificó en el sistema Isolucion el formato CA-F-015 Acuerdo de Confidencialidad y Aceptación de Políticas de Seguridad de la Información; no obstante, en el Manual de Políticas de Seguridad de la Información no se establecen los lineamientos que definan las instancias en las que dicho formato debe ser utilizado o diligenciado. En este sentido, se recomienda incorporar esta información en la documentación correspondiente, complementar las evidencias que soportan la implementación del control y registrar en el campo de brechas los aspectos pendientes que permitan alcanzar el nivel esperado de cumplimiento.
AD.1.21	A 5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC	80	Para el control de Gestión de la seguridad de la información en la cadena de suministro de las TIC, la dependencia asignó 80 puntos y relacionó como seguimiento que el manual define los requisitos a incluir en los acuerdos con proveedores y contratistas. Esta previsión es general y no aborda de manera directa el objeto del control ni referencia el procedimiento vigente. Se identifica que el procedimiento TI-P-010, numeral 4.3, desarrolla la gestión de proveedores de TIC a lo largo de todo el ciclo de vida precontractual, contractual y poscontractual, con evaluación de riesgos, anexos de seguridad y derecho de auditoría, lineamientos que no fueron referenciados en el instrumento. Se observa además que el campo de brecha no fue diligenciado, por lo que se recomienda referenciar el procedimiento TI-P-010, aportar la evaluación de riesgo de un proveedor crítico de TIC, revalidar la calificación asignada y precisar en el instrumento los aspectos pendientes.

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
AD.1.22	A 5.22	Seguimiento, Revisión y Gestión de Cambios de Servicios de Proveedores	80	La evidencia se concentra en el Procedimiento de Gestión de Cambios Tecnológicos (código APO4-P-010, citado en el instrumento), que atiende la gestión de los cambios en los servicios de proveedores prevista en el literal c del numeral 4.30.2 del manual. No obstante, no se acredita el seguimiento y la revisión periódica de los servicios de proveedores, exigidos en la última cláusula del literal b de este numeral. Se observa que el campo de brecha no fue diligenciado, por lo que se recomienda aportar los registros de seguimiento y revisión de los servicios de proveedores y precisar los aspectos pendientes.
AD.1.23	A 5.23	Seguridad de la información para el uso de servicios en la nube	60	Se identifica que el campo de evidencia es genérico, limitándose a señalar que "se mantienen controles en Nube", sin sustentar el control. Al contrastar lo declarado con el manual de políticas, este no desarrolla una política específica para el uso de servicios en la nube, control nuevo en la NTC-ISO/IEC 27001:2022. Pese a ello, se otorgó una calificación de 60 puntos sin que el campo de brecha precise los aspectos pendientes. Se recomienda revalidar la calificación, formalizar la política de uso de servicios en la nube y aportar los acuerdos y controles establecidos con los proveedores cloud.
AD.1.24	A 5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	100	La evidencia aportada para este control corresponde al Procedimiento de Gestión de Incidentes de Seguridad de la Información (código APO4-P-007), único documento citado en el campo de evidencia del instrumento. Dicho procedimiento desarrolla la política establecida en el numeral 4.31 (Gestión de Incidentes de Seguridad de la Información) del Manual de Políticas de Seguridad de la Información (APO4-M-002 V2). De manera complementaria, se identifica dentro del SIG el documento EG-P-003 (Gobierno de Seguridad de la Información y Continuidad del Servicio Tecnológico) aborda, en su numeral de roles y responsabilidades, la comunicación con la Alta Dirección frente a los incidentes críticos.

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
AD.1.25	A 5.25	Evaluación y Decisión sobre Eventos de Seguridad de la Información	80	Para el control de Evaluación y decisión sobre eventos de seguridad de la información, la evidencia describe la categorización de incidentes por afectación a la confidencialidad, integridad o disponibilidad, en línea con el numeral 4.31 del manual. Aranda y CAST corresponden a la misma herramienta de mesa de ayuda: Aranda es la versión anterior, habilitada solo para consulta, y CAST la versión actual, empleada para la gestión de incidentes. Se aportaron los reportes de Aranda (14.239 casos, del 1 de enero al 12 de mayo de 2025) y de CAST (23.662 casos, del 12 de mayo al 31 de diciembre de 2025). De la revisión del reporte de CAST se observa que 1.555 casos corresponden al tipo (Incidente), de los cuales el 76 % cumplió el Acuerdo de Niveles de Servicio (ANS) y el 23 % no lo cumplió; a nivel general, el 15,3 % de los 23.662 casos registró incumplimiento del ANS. Se recomienda realizar un seguimiento a los casos con incumplimiento de ANS, para así sustentar el cumplimiento total del control.
AD.1.26	A 5.26	Respuesta a los Incidentes de Seguridad de la Información	100	Como seguimiento al control, la información dentro del instrumento indica que la entidad cuenta con el Procedimiento de Gestión de Incidentes de Seguridad de la Información (código APO4-P-007), en línea con el numeral 4.31 (Gestión de Incidentes de Seguridad de la Información) del Manual de Políticas de Seguridad de la Información (APO4-M-002 V2); no obstante, y de acuerdo con lo validado, esta acredita la existencia del procedimiento. Se recomienda aportar evidencia de la gestión de incidentes tal como lo indica tanto el manual como el procedimiento.
AD.1.27	A 5.27	Aprendizaje sobre los incidentes de seguridad de la información	80	En referencia a aprendizaje sobre los incidentes de seguridad de la información, se identifica que la evidencia no acredita la cuantificación y el monitoreo de los tipos, volúmenes y costos de los incidentes que la prueba relaciona, pese a que la entidad dispone de información en las herramientas Aranda y CAST. El numeral 4.31 del manual prevé el aprendizaje a partir de los incidentes. Se observa que el campo de brecha no fue diligenciado, por lo que se recomienda precisar los aspectos pendientes para llegar a la calificación de 100.

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
AD.1.28	A 5.28	Recopilación de pruebas	80	Se identifica por parte del equipo auditor que el campo de evidencia es idéntico al diligenciado para el control 5.27 (Aprendizaje sobre los incidentes) y no aborda los aspectos propios de este control, relativos a la identificación, recolección, adquisición y preservación de evidencia digital con fines disciplinarios y legales (informática y análisis forense, numerales 3.34 y 3.50 del manual). Se observa que el campo de brecha no fue diligenciado pese a la calificación de 80 puntos. Se recomienda revalidar la calificación y precisar los aspectos pendientes.
AD.1.29	A 5.29	Seguridad de la información durante la interrupción	80	Respecto al control de Seguridad de la información durante la interrupción, la evidencia indica la existencia de un DRP a nivel de infraestructura, en línea con el numeral 4.33 del manual. Se identifica que no se aportaron el Plan de Continuidad ni el BIA que articulen los controles de seguridad durante la interrupción, documentos que no fueron suministrados a esta auditoría. Se observa que el campo de brecha no fue diligenciado, por lo que se recomienda aportar dichos documentos y relacionar los aspectos pendientes.
AD.1.30	A 5.30	Preparación de las TIC para la continuidad del negocio	60	En referencia al control Preparación de las TIC para la continuidad del negocio, se identifica una inconsistencia, toda vez que el propio campo de evidencia del instrumento reconoce, textualmente, que "se realizan pruena [sic] del PRD anual. Pero es insuficiente para la infraestructura de la ANM". El numeral 4.33.2 del manual exige establecer el DRP y realizar sus pruebas periódicas. Pese a la insuficiencia declarada por la propia OTI, se otorgó una calificación de 60 puntos sin que el campo de brecha precise las acciones pendientes. Se recomienda revalidar la calificación, aportar documentación asociada y describir los temas o actividades a desarrollar para alcanzar la calificación de 100.
AD.1.31	A 5.31	Requisitos legales, estatutarios, reglamentarios y contractuales	100	Para el tema de Requisitos legales, estatutarios, reglamentarios y contractuales, la entidad publica en su portal el Normograma consolidado por semestres, actualizado al Primer Semestre 2026, que incorpora disposiciones como la Ley 1712 de 2014, la Resolución 500 de 2021 del MinTIC, el Decreto 1078 de 2015 y el Decreto 767 de 2022. Se observa que el Normograma no referencia la la Ley 603 de 2000, esta

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
				última citada en la evidencia del instrumento. Adicionalmente, en la subsección (Leyes) del portal, la norma más reciente publicada corresponde a la Ley 1882 de 2018. Se recomienda incorporar dichas disposiciones al Normograma y actualizar el repositorio de leyes publicado.
AD.1.32	A 5.32	Derechos de propiedad intelectual	100	En el seguimiento al control de Derechos de Propiedad Intelectual, la evidencia reportada por la OTI señala que el licenciamiento del software es gestionado por la dependencia, existen controles para prevenir la instalación de software no autorizado y se incluyen cláusulas de derechos de autor en los contratos, conforme a los numerales 4.25 y 4.34.2 del Manual de Políticas de Seguridad de la Información, lo que soportó la calificación de 100 puntos. Sin embargo, en la presente vigencia la Oficina de Control Interno, mediante el Informe de Derechos de Autor ANM-OCI-008-2026, evidenció situaciones asociadas a la instalación de software que deben ser consideradas en la valoración del control. Por lo anterior, se recomienda revisar la calificación otorgada y complementar las evidencias con los resultados de las revisiones periódicas previstas en el Manual.
AD.1.33	A 5.33	Protección de registros	60	El equipo auditor identifica para el control de Protección de registros, que la evidencia se apoya en el procedimiento de descripción documental APO7-P-010, propio del proceso de Gestión Documental, y no en los controles de seguridad de la información que el control relaciona (protección de la autenticidad, confiabilidad, integridad y disponibilidad de los registros, directrices de almacenamiento y tiempos de retención, numeral 4.34.3 del manual). Pese a ello, se otorgó una calificación de 60 puntos sin que el campo de brecha precise los aspectos pendientes. Se recomienda revalidar la calificación y aportar la evidencia de los controles de seguridad sobre los registros.

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
AD.1.34	A 5.34	Privacidad y protección de la PII	100	Para el control de Privacidad y protección de la información de datos personales PII (Personally, Identifiable and Information), la evidencia se soporta en la Política de Protección de Datos Personales, la Política de Privacidad y Términos de Uso publicadas en el portal web, el rol de Oficial de Protección de Datos Personales y el numeral 4.34.4 del manual (Ley 1581 de 2012), lo cual sustenta la calificación de 100 puntos. Se recomienda verificar la vigencia de las políticas publicadas y el registro de las bases de datos ante la autoridad competente.
AD.1.35	A 5.35	Revisión independiente de la seguridad de la información	80	En el seguimiento al control de Revisión independiente de la seguridad de la información, el numeral 4.35.1 del manual asigna las auditorías internas de revisión independiente al SGSI al proceso de Evaluación, Control y Mejora, y precisa que son responsabilidad de Control Interno de la ANM. Se identifica que la evidencia las vincula al plan de auditorías de la Oficina de Planeación; y el proceso se registra como (Evaluación, Control y Mejora) en el manual y como (Evaluación, Seguimiento y Mejora) en Isolucion, lo que constituye una inconsistencia de denominación. El campo de brecha no fue diligenciado. Se recomienda actualizar el nombre del proceso en los documentos oficiales y determinar las actividades faltantes para obtener calificación de 100.
AD.1.36	A 5.36	Cumplimiento de políticas, normas y estándares de seguridad de la información	80	Para el tema de Cumplimiento de las políticas, normas y estándares de seguridad de la información, la evidencia se respalda en el plan de sensibilización del SGSI, en las revisiones de Control Interno y en el Plan de Socialización SI-TIC 2026 aportado, que proyecta 592 asistentes en uso y apropiación e incluye el dominio de Seguridad, en línea con el numeral 4.35.2 del manual. La calificación de 80 puntos resulta razonable; no obstante, se observa que el campo de brecha no fue diligenciado. Se recomienda referenciar el Plan de Socialización SI-TIC 2026 y los informes de revisión de cumplimiento, y precisar los aspectos pendientes.

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
AD.1.37	A 5.37	Procedimientos operativos documentados	80	En el seguimiento al control de Procedimientos operativos documentados, la evidencia relaciona procedimientos de la OTI, en línea con el numeral 4.21.1 del manual. Se identifican procedimientos citados fueron recodificados en noviembre de 2025: la Gestión de Vulnerabilidades quedó integrada en el procedimiento TI-P-010 y la Gestión de Capacidad, anteriormente APO4-P-008, fue reemplazada en el nuevo proceso de Estrategia y Gobierno de TIC (EG-P-001). Se observa que el campo de brecha no fue diligenciado, por lo que se recomienda actualizar las referencias documentales a los códigos vigentes del sistema integrado de gestión y precisar los aspectos pendientes.

Fuente: Matriz de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), diligenciada por la Oficina de Tecnologías de la Información (OTI) - 2026.

6.4. Dominio controles de personas:

En la Tabla 3 se relacionan las observaciones de la Oficina de Control Interno sobre los controles de personas del Anexo A.

Tabla 3 Seguimiento a la efectividad de los controles de personas - Observaciones de la Oficina de Control Interno.

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
P.1.1	A 6.1	Revisión de antecedentes	100	Se identifica que el campo de evidencia reconoce que *"no se cuenta con acuerdos de confidencialidad para usuarios de planta"*. La verificación de antecedentes se encuentra a cargo del Grupo de Contratación conforme al numeral 4.10.2 del manual. Esta ausencia parcial de control no resulta consistente con una calificación de 100 puntos, nivel que corresponde a un control consolidado y plenamente operativo. Por lo indicado, se recomienda revalidar la calificación teniendo en cuenta lo descrito.

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
P.1.2	A 6.2	Términos y condiciones de empleo	80	Para el tema de Términos y condiciones de empleo, la evidencia se soporta en el procedimiento de ejecución contractual APO1-P-001-I-002, el paz y salvo y los formatos de entrega de cargo, en línea con los numerales 4.10.1 y 4.10.4 del manual, que exigen incluir las responsabilidades de seguridad en los acuerdos contractuales. La calificación de 80 puntos resulta razonable; no obstante, se observa que el campo de brecha no fue diligenciado. Se recomienda aportar evidencias asociadas donde consten las cláusulas de seguridad de la información y precisar los aspectos pendientes para tener calificación de 100.
P.1.3	A 6.3	Concientización, educación y entrenamiento en seguridad de la información	100	En el seguimiento al control de Concientización, educación y entrenamiento, la evidencia describe la inducción, reinducción y charlas periódicas de sensibilización, en concordancia con el numeral 4.10.4 literales e y f del manual, y queda respaldada en el Plan de Socialización SI-TIC 2026 aportado, que proyecta 592 asistentes en uso y apropiación e incluye el dominio de Seguridad. La evidencia resulta consistente con la calificación de 100 puntos. Se recomienda conservar los registros de asistencia como evidencia de ejecución del programa.
P.1.4	A 6.4	Proceso disciplinario	80	Para el control de Proceso disciplinario, se identifica que el propio campo de evidencia reconoce que "*no se tiene establecido proceso disciplinario formal por manejo indebido de la información*". El numeral 4.10.6 del manual remite de manera general a la Ley 734 de 2002, sin desarrollar un procedimiento disciplinario específico para violaciones de seguridad de la información. Pese a la brecha reconocida, se otorgó una calificación de 80 puntos sin que el campo de brecha precise los aspectos pendientes. Se recomienda formalizar el proceso disciplinario aplicable a las violaciones de seguridad, articulándolo con la gestión de incidentes y establecer las actividades o documentación asociada para obtener la calificaciones 100 puntos.
P.1.5	A 6.5	Responsabilidades después de la finalización o cambio de empleo	80	El equipo auditoria identifica en el tema de Responsabilidades después de la finalización o cambio de empleo, la evidencia se soporta en el procedimiento APO1-P-001-I-002, el paz y salvo y las actas de entrega de cargo, en concordancia con el numeral 4.10.5 del manual. No obstante, se observa que el campo de brecha no fue diligenciado. Se recomienda aportar evidencia de la revocación de accesos asociada al retiro (numeral 4.17.4) y precisar los aspectos pendientes.

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
P.1.6	A 6.6	Acuerdos de confidencialidad o no divulgación	80	Respecto a los Acuerdos de confidencialidad o no divulgación, la evidencia se soporta en las cláusulas contractuales (APO1-P-001-F-030) y en el formato de Acuerdo de Confidencialidad y Aceptación de la Política de Seguridad de la Información (CA-F-015) aportado, en línea con los numerales 4.10.4 y 4.28.2 del manual. Se identifica que la propia evidencia indica que el acuerdo "*actualmente se estructura con el Grupo de Contratación*", situación consistente con la brecha del control 6.1 para el personal de planta. Se observa que el campo de brecha no fue diligenciado, por lo que se recomienda formalizar y desplegar el acuerdo CA-F-015 para todo el personal, incluido el de planta e indicar cuales son las actividades o entregables para cumplir con una calificación de 100.
P.1.7	A 6.7	Trabajo remoto	100	En el seguimiento al control de Trabajo remoto, la evidencia describe el uso de ZTNA, el control de las políticas de conexión remota y las auditorías de conectividad, en concordancia con el numeral 4.9 del manual y el numeral 4.5 del procedimiento TI-P-010, lo cual sustenta la calificación de 100 puntos. Se recomienda conservar los registros de validación de la postura de seguridad de los equipos remotos como evidencia de operación del control.
P.1.8	A 6.8	Reporte de eventos de seguridad de la información	100	En el seguimiento al control de Reporte de eventos de seguridad de la información, la evidencia describe el reporte mediante mesa de ayuda y las herramientas Aranda (14.239 casos entre enero y mayo de 2025) y CAST (23.662 casos entre mayo y diciembre de 2025), en concordancia con el numeral 4.31.1 del manual. La evidencia resulta consistente con la calificación de 100 puntos, si bien las herramientas citadas corresponden a mesa de ayuda general. Se recomienda conservar evidencia de la socialización de los canales de reporte y diferenciar los eventos de seguridad dentro del universo de casos.

Fuente: Matriz de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), diligenciada por la Oficina de Tecnologías de la Información (OTI), elaboración propia comentarios y análisis de la Oficina de Control Interno

6.5. Dominio controles físicos:

En la Tabla 4 se relacionan las observaciones de la Oficina de Control Interno sobre los controles físicos del Anexo A.

Tabla 4 Seguimiento a la efectividad de los controles físicos – Observaciones de la Oficina de Control Interno.

ID.ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
F.1.1	A 7.1	Perímetros de seguridad física	80	Para este control, se cita el procedimiento de vigilancia y seguridad privada y los controles de acceso al centro de procesamiento de datos y al Rack, en línea con el numeral 4.20 del manual. Se observó que el control fue valorado con 80 puntos; no obstante, el campo correspondiente a brechas no incorpora los aspectos pendientes que soportan la diferencia respecto del cumplimiento total. Dado que el registro de brechas constituye el insumo para la gestión y seguimiento de las acciones de mejora, es importante que en este se consignen de manera expresa los controles o actividades aún por implementar para alcanzar el nivel de madurez esperado.
F.1.2	A 7.2	Entrada física	100	Se evidenció que el proceso otorgó una calificación de 100 puntos, sustentada en la existencia de controles de acceso físico, entre ellos el uso de carné institucional, el registro de visitantes y la prestación del servicio de seguridad y vigilancia. No obstante, durante la verificación se observó que no todo el personal portaba o contaba con carné de identificación institucional. Asimismo, el documento APO4-M-002 Políticas de Seguridad de la Información V2 no establece lineamientos para la gestión de este control, por lo que se considera pertinente evaluar su incorporación o definirlos en el instrumento correspondiente.
F.1.3	A 7.3	Aseguramiento de oficinas, salas e instalaciones	100	Respecto al control de aseguramiento de oficinas, salas e instalaciones, la evidencia presentada describe los controles de acceso a oficinas, archivadores de historias laborales y racks, en concordancia con los numerales 4.20.1 y 4.20.2 del Manual de Políticas de Seguridad de la Información, lo que sustenta la calificación de 100 puntos. No obstante, se considera conveniente fortalecer los soportes que evidencien la implementación y operación del control, mediante registros, bitácoras u otros mecanismos que permitan verificar su aplicación y seguimiento.

ID.ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
F.1.4	A 7.4	Supervisión de la seguridad física	80	Para este control, el equipo auditor observa que el proceso responsable no reporta en el instrumento información que indique cómo se da cumplimiento a este control, dejando el campo de evidencia sin diligenciar. Al contrastar lo anterior con el manual de políticas, este desarrolla el sistema de CCTV en el numeral 4.20.1 (monitoreo permanente a cargo del Grupo de Servicios Administrativos, bitácora diaria, restricción del centro de monitoreo y retención de las grabaciones), aspectos que no fueron referenciados en el instrumento. Pese a la ausencia de evidencia, se otorgó una calificación de 80 puntos sin que el campo de brecha precise los aspectos pendientes. Se recomienda diligenciar el campo de evidencia con el soporte del CCTV y revalidar la calificación otorgada.
F.1.5	A 7.5	Protección contra amenazas físicas y ambientales	80	En el instrumento para este control, se valida que la evidencia reportada en el instrumento contempla las edificaciones sismorresistentes, el sistema de pararrayos, el sistema contra incendio y las buenas prácticas ISO 14001:2015, conforme al numeral 4.20 del manual. Sin embargo, aunque la calificación de 80 puntos guarda relación con lo verificado, el campo de brecha permanece sin diligenciar, por lo que no se detallan los aspectos aún pendientes. Se recomienda complementar la evidencia con la evaluación de riesgos físicos y ambientales y dejar claramente establecidos los requerimientos faltantes.
F.1.6	A 7.6	Trabajar en áreas seguras	80	Como resultado de la verificación del control de Trabajar en áreas seguras, la evidencia aportada relaciona los extintores y aires acondicionados, en concordancia con los requisitos ambientales del centro de procesamiento de datos previstos en el numeral 4.20.1 del manual. No obstante, se observa que el campo de brecha no fue diligenciado siendo que la calificación otorgada fue de 80, por tanto, se recomienda precisar los aspectos pendientes y registrarlos en el instrumento para la siguiente evaluación.

ID.ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
F.1.7	A 7.7	Escritorio despejado y pantalla despejada	80	Al revisar el control de Escritorio despejado y pantalla despejada, se observa que la evidencia reportada hace referencia a la política de equipo desatendido, escritorio limpio y pantalla limpia establecida en el numeral 4.20.8 del manual. Sin embargo, el campo de brecha no fue diligenciado siendo que la calificación fue de 80 puntos, razón por la cual no se identifican con claridad los aspectos pendientes. Se recomienda soportar con evidencia de los controles actualmente implementados y precisar los requerimientos faltantes.
F.1.8	A 7.8	Ubicación y Protección del equipo	100	En el seguimiento al control de Ubicación y protección del equipo, la evidencia describe los esquemas de seguridad en las áreas de procesamiento de datos y la protección de los equipos en los PAR, en concordancia con el numeral 4.20.2 del manual. Para posteriores mediciones se recomienda asociar evidencia objetiva que acredite la operación efectiva del control, con el fin de fortalecer la trazabilidad y el proceso de evaluación.
F.1.9	A 7.9	Seguridad de los activos fuera de las instalaciones	80	Respecto del control de Seguridad de los activos fuera de las instalaciones, la evidencia registrada en el instrumento MSPI cita los lineamientos del numeral 4.20.6 del manual y el instructivo de entrega de equipos para trabajo en casa, con lo cual se acredita el soporte documental del control. Se observa que el campo de brecha no fue diligenciado, por lo que se recomienda relacionar las evidencias que den cumplimiento al control conforme a lo establecido y registrar en dicho campo los aspectos pendientes para alcanzar el cumplimiento total.
F.1.10	A 7.10	Medios de almacenamiento	100	Para el control de Medios de almacenamiento se identifica una inconsistencia en la referencia documental, toda vez que el instrumento cita el numeral 4.8.7, mientras que la gestión de medios removibles se desarrolla en el numeral 4.15 del manual de políticas vigente (V2, diciembre de 2024), que contempla el cifrado, el bloqueo por directorio activo y la autorización para su uso. Se recomienda corregir la referencia documental al numeral 4.15 del manual y precisar en el instrumento los aspectos pendientes.

ID.ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
F.1.11	A 7.11	Servicios de apoyo	80	En el seguimiento realizado al control de Servicios de apoyo, la evidencia cita dos UPS, la planta eléctrica con transferencia automática y el respaldo en los PAR, en concordancia con el numeral 4.20.3 del manual. No obstante, se observa que el campo de brecha no fue diligenciado, por tanto, se recomienda aportar los registros de prueba de la planta eléctrica y de las UPS y precisar los aspectos pendientes para el total cumplimiento.
F.1.12	A 7.12	Seguridad del cableado	100	En el seguimiento al control de Seguridad del cableado, la evidencia describe el cableado estructurado y los switches de borde y de core asegurados, en concordancia con el numeral 4.20.4 del manual (estándar ISO/IEC 11801), lo cual sustenta la calificación de 100 puntos. Se recomienda aportar la documentación del cableado estructurado y sus certificaciones para los ejercicios de auditoría y seguimiento realizados con el cual se respalde la calificación otorgada.
F.1.13	A 7.13	Mantenimiento de equipos	100	En el seguimiento al control de Mantenimiento de equipos, la evidencia cita los esquemas de mantenimiento preventivo, en concordancia con el numeral 4.20.5 del manual y el formato de informe de servicio. Se recomienda aportar el plan anual de mantenimiento y sus registros de ejecución como evidencia de operación del control.
F.1.14	A 7.14	Eliminación segura o reutilización de equipos	80	En el seguimiento al control de Eliminación segura o reutilización de equipos, la evidencia cita los lineamientos de disposición segura o reutilización de equipos del numeral 4.20.7 del manual (borrado seguro). La calificación de 80 puntos resulta razonable; no obstante, se observa que el campo de brecha no fue diligenciado. Se recomienda aportar el procedimiento y los registros de borrado seguro y precisar los aspectos pendientes.

Fuente: Matriz de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), diligenciada por la Oficina de Tecnologías de la Información (OTI) - 2026.

6.6. Dominio controles Tecnológicos:

En la Tabla 5 se relacionan las observaciones de la Oficina de Control Interno sobre los controles tecnológicos del Anexo A.

Tabla 5 Seguimiento a la efectividad de los controles tecnológicos – Observaciones de la Oficina de Control Interno.

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
T.1.1	A 8.1	Dispositivos de punto final de usuario	100	En el seguimiento al control se identifica que el campo de evidencia del instrumento MSPI no sustenta la totalidad de los aspectos que la propia prueba relaciona para este control, limitándose a citar el numeral 4.8.7 del manual de políticas de seguridad de la información sobre medios removibles. No obstante, el manual cuenta con lineamientos adicionales para varios de estos aspectos, tales como requisitos específicos de antivirus, firewall, control web, acceso controlado a carpetas y protección de identidad descritos en el numeral 4.8, Política de Uso de Dispositivos No Corporativos, que no fueron referenciados en el instrumento. En consecuencia, se recomienda revalidar la calificación de 100 puntos otorgada y ampliar en el instrumento la información sobre cómo se aborda el control en la entidad.
T.1.2	A 8.2	Derechos de acceso privilegiado	80	Se identifica que el instrumento MSPI no sustenta de manera integral los aspectos que la prueba sugiere para este control, relacionados con la gestión, autorización, seguimiento y revisión de los accesos con privilegios especiales, limitándose a citar el Directorio Activo, el procedimiento de control de acceso mediante formato IMAC y un numeral del manual de políticas que, al verificarse, resulta desactualizado frente a la versión vigente del documento (V2, diciembre de 2024). Al contrastar lo declarado con la totalidad del manual de políticas de seguridad de la información, se identifica que este sí desarrolla lineamientos relevantes para la gestión de cuentas y accesos privilegiados, incluyendo la custodia y delegación de usuarios administradores, el monitoreo de cuentas privilegiadas y la restricción de identificadores genéricos, los cuales no fueron referenciados en el instrumento, limitando la trazabilidad de la evidencia frente a lo declarado. Se observa también que el campo de brecha no fue diligenciado. Por lo indicado, se recomienda actualizar la referencia documental, referenciar los numerales vigentes del manual y diligenciar el campo de brecha relacionando los

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
				aspectos pendientes para alcanzar el cumplimiento total del control.
T.1.3	A 8.3	Restricción de acceso a la información	80	El campo de evidencia del instrumento no sustenta de manera integral el control, ya que se limita a una referencia genérica a la política de control de acceso, sin especificar los mecanismos de restricción, gestión dinámica de acceso o cifrado que la entidad tiene implementados. El manual de políticas desarrolla lineamientos concretos sobre permisos de lectura, escritura, modificación y eliminación, restricción de impresión de documentos confidenciales y acceso temporal controlado. Adicionalmente, el Plan de Tratamiento de Riesgos 2026 y el indicador de prevención de fuga de datos respaldan el uso de herramientas como Azure Active Directory, Intune y EMS E3 para la gestión dinámica de acceso. En consecuencia, aunque la calificación de 80 puntos resulta razonable frente a la implementación real, es importante que en el campo de brecha del instrumento se indique de manera puntual qué aspectos faltan por implementar o documentar para alcanzar el cumplimiento total del control.
T.1.4	A 8.4	Acceso al código fuente	60	La respuesta se limita a mencionar de forma general los lineamientos de desarrollo y soporte, sin precisar cómo se controla realmente el código fuente. El manual desarrolla aspectos concretos como aplicar los mismos controles de acceso entre desarrollo y producción, autorizar modificaciones mediante gestión de cambios y contar con un sistema de control de versiones, ninguno de los cuales quedó citado. Si bien se otorgó una calificación de 60 puntos, se recomienda describir en el campo de brecha del instrumento qué aspectos faltan por implementar o documentar para alcanzar el cumplimiento total del control.

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
T.1.5	A 8.5	Autenticación segura	100	La evidencia reportada señala que los mecanismos de doble factor de autenticación están en proceso de implementación, lo que no justifica una calificación de 100 puntos. En la documentación se identificaron lineamientos para bloqueo automático, registro de intentos de acceso y cierre de sesiones inactivas, pero falta el aviso de advertencia previo al ingreso. En la auditoría a generación de títulos mineros y específicamente al sistema de información ANNA Minería fueron identificados usuarios sin vínculo laboral o contractual con cuentas aún activas. También, se debe precisar en el campo de brecha qué elementos faltan para sostener dicho nivel de cumplimiento. Ante lo anterior, se sugiere validar la calificación otorgada.
T.1.6	A 8.6	Gestión de la capacidad	60	La evidencia aportada se refiere a las pruebas del DRP con apoyo del SOC, que corresponden a continuidad del negocio y no a la gestión de capacidad. El numeral 4.21.3 del manual exige gestionar la capacidad de la plataforma según el procedimiento APO4-P-008, código que no fue posible ubicar en el sistema de gestión. Tampoco se hallaron registros de monitoreo de recursos clave, proyecciones de necesidades futuras ni un plan documentado de capacidad para los sistemas críticos. Se recomienda registrar en el campo de brecha los aspectos que faltan para completar el control.
T.1.7	A 8.7	Protección contra malware	80	Si bien la entidad cuenta con herramienta antivirus McAfee Endpoint y desarrolla capacitaciones de sensibilización según lo reporta la OTI, la evidencia reportada en el instrumento no cubre la totalidad de los aspectos que sustentan este control. La documentación suministrada permitió identificar soporte adicional en la gestión de vulnerabilidades técnicas, los filtros de contenido web y las copias de respaldo asociadas a la recuperación de incidentes. Adicionalmente, si bien se otorgó una calificación de 80 puntos, no se reporta dentro del campo de brecha cuáles son los aspectos pendientes para alcanzar el cumplimiento total del control.

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
T.1.8	A 8.8	Gestión de vulnerabilidades técnicas	100	La evidencia reportada por la OTI cita el procedimiento APO4-P-013, código que no se encuentra asociado en el sistema integrado de gestión. La gestión de vulnerabilidades se identifica como una actividad dentro del procedimiento EG-P-003, el cual contempla como producto formal un Plan de Gestión y Tratamiento de Vulnerabilidades, documento que se debe verificar dentro del sistema integrado de gestión. Se recomienda actualizar la referencia documental del instrumento y detallar de manera puntual la respuesta frente a cada uno de los aspectos relacionados con la prueba del control.
T.1.9	A 8.9	Gestión de la configuración	60	El proceso responsable dejó el campo de evidencia sin diligenciar, pese a lo cual el control recibió 60 puntos y la brecha tampoco precisa qué falta. Vale la pena revisar de nuevo esa calificación y aterrizarla con información puntual sobre las plantillas de configuración segura, los registros de cambios y el monitoreo de desviaciones frente a la configuración definida, de modo que refleje el nivel real de cumplimiento.
T.1.10	A 8.10	Eliminación de información	60	Igual que en el control anterior, el campo de evidencia quedó vacío y la calificación de 60 puntos no está respaldada ni acompañada de una brecha que aclare lo pendiente. Conviene revisar la calificación y puntualizar los métodos de eliminación segura, los registros que la evidencien y el tratamiento dado a la información en manos de proveedores y servicios en la nube, además de relacionar los lineamientos que ya existen en el sistema de gestión sobre el tema.
T.1.11	A 8.11	Enmascaramiento de datos	60	La OTI tampoco diligenció el campo de evidencia y, aun así, el control quedó en 60 puntos sin que la brecha explique lo faltante. Se sugiere revisar la calificación y detallar las técnicas aplicadas para proteger la información sensible; en línea con la prueba, la entidad debería definir e implementar mecanismos de enmascaramiento, seudonimización o anonimización, junto con los controles de acceso y uso que correspondan.

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
T.1.12	A 8.12	Prevención de fuga de datos	80	La evidencia reportada por la OTI indica que se ha dado inicio a medidas de control Data Loss Prevention y políticas de fuga de datos en MS 365, lo cual no resulta consistente con una calificación de 80 puntos, nivel que corresponde a un control gestionado y en operación sostenida. El manual de políticas hace referencia a la protección de copias de seguridad mediante cifrado y control de acceso. Se recomienda revalidar la calificación otorgada conforme al estado real de madurez declarado por la OTI. En línea con lo señalado por la prueba del instrumento, se sugiere que la entidad articule y documente las medidas de prevención de fuga de datos apoyándose en las capacidades de trazabilidad ya disponibles en herramientas institucionales, entre otros mecanismos de monitoreo y control existentes en la plataforma tecnológica de la ANM.
T.1.13	A 8.13	Copia de seguridad de la información	80	La OTI cita el código APO4-P-004-I-001, que no está vigente; los procedimientos actuales TI-P-009 y TI-I-004 fijan copias completas semanales y copias de cambios diarias según la importancia de la información. En ANNA Minería se confirmó que los respaldos se hacen de forma automática, se guardan en un almacenamiento externo con redundancia de dos servidores activos, se verifican periódicamente y cuentan con ejercicios de recuperación documentados. No obstante, la propia OTI reconoce que esas copias no se envían a un centro de datos alterno, lo que incumple el numeral 4.23 del manual. Se recomienda actualizar las referencias del instrumento y dejar en la brecha los aspectos que faltan para cerrar el control.
T.1.14	A 8.14	Redundancia de las instalaciones de procesamiento de información	80	Se cita el código APO4-P-004-I-001, ya no vigente. Los procedimientos TI-P-009 y TI-I-004 contemplan respaldo diferenciado por importancia, copia automática entre el centro de datos principal y uno alterno, monitoreo de las copias, ejercicios de recuperación y política de retención para Microsoft 365, y el manual añade lineamientos de protección física de los medios y su relación con la continuidad del negocio. Sin embargo, en ANNA Minería se verificó que, si bien hay redundancia local de dos servidores activos con verificación periódica, los respaldos no se replican a un datacenter alterno, lo que contraviene el

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
				numeral 4.23. Conviene actualizar las referencias y precisar en la brecha lo que falta para cumplir del todo.
T.1.15	A 8.15	Registro	80	La OTI reporta que los registros se guardan según el sistema de gestión documental, declaración insuficiente para un control que exige política específica, catálogo de eventos, revisión periódica y protección contra alteraciones. En la documentación revisada se confirmó que el manual de políticas establece el registro de logs como requisito y que se mantiene registro en los sistemas críticos de la ANM; sin embargo, la Declaración de Aplicabilidad reconoce que la revisión de logs no se realiza periódicamente sino solo cuando hay investigación de incidentes. Además, en la hoja "Cumplimiento v2013" del SOA_ANM-2025.xlsx (filas 97, 98 y 99) se registran como tareas pendientes la verificación de configuraciones con el proveedor RENATA, la validación de controles de protección en aplicaciones y bases de datos, y la reactivación del registro de actividades de administrador. El plan de seguridad para 2026 contempla la auditoría de logs y gestión de cumplimiento normativo como actividades aún por ejecutarse. Aunque el campo de brecha del instrumento tiene un registro, solo menciona documentar y establecer periodicidad, sin cubrir los demás aspectos faltantes. Se sugiere revalidar la calificación asignada detallando en el campo brecha los aspectos que faltan para cumplir completamente con este control.
T.1.16	A 8.16	Actividades de seguimiento	80	La OTI indica en el instrumento que se cuenta con herramientas internas de monitoreo y un SOC, pero no precisa cuáles ni con qué periodicidad operan. El SOA 2025 y 2026 (fila 104) confirma el servicio de SOC externo, aunque la misma hoja (fila 97) reconoce que la revisión de logs solo se hace ante incidentes, situación que no cambió entre ambas vigencias, y el manual (numeral 4.9.4, literal a) deja como pendiente reforzar el monitoreo para detectar accesos indebidos o situaciones anormales. Falta relacionar en la brecha los aspectos que permitan completar el control.
T.1.17	A 8.17	Sincronización del reloj (clock)	100	Se reporta en el instrumento MSPI que la sincronización de relojes de toda la plataforma tecnológica se realiza con el Instituto Nacional de Metrología de Colombia, lo cual coincide con lo registrado en la Declaración de Aplicabilidad. Sin embargo, el archivo Cronograma Plan Networking.xlsx programa como proyecto para el tercer trimestre de 2026 el

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
				"Aseguramiento DNS/NTP" con autenticación NTP, actividad aún no ejecutada que compromete la protección del mecanismo de sincronización frente a manipulación. En el instrumento se reporta una calificación de 100 sin que se acredite la fuente documental que soporta dicha calificación ni se contemple esta actividad pendiente de aseguramiento, ante lo descrito se sugiere acreditar la fuente documental que la soporta y contemplar esa actividad pendiente.
T.1.18	A 8.18	Uso de programas de utilidad privilegiados	100	El control se sustenta en la Ley 603 de 2000, que trata de derechos de autor de software y no del objeto real del control, que es restringir los programas capaces de anular los controles del sistema. El numeral aplicable es el 4.18.4 del manual, que pide restringir esos programas, mantener un inventario, limitar su uso a personal autorizado, registrar cada uso y documentar los niveles de autorización. La Declaración de Aplicabilidad (fila 62) apenas señala que la OTI controla estos programas, sin evidenciar inventario, registro ni niveles de autorización. Se recomienda revisar la calificación y aportar la evidencia que realmente sustente el cumplimiento.
T.1.19	A 8.19	Instalación de software en sistemas operativos	100	La OTI presenta la misma evidencia del control A 8.18 y no aporta el procedimiento de control de cambios e instalación de software en sistemas operativos que el control exige, pese a que el manual tiene un numeral específico sobre el asunto. Conviene revisar la calificación y reorientar la respuesta del instrumento hacia ese lineamiento interno y hacia la forma concreta en que la entidad cumple el control.
T.1.20	A 8.20	Seguridad en redes	80	La OTI menciona la segmentación de la red, las políticas del manual y los procedimientos de administración de infraestructura, pero sin citar el código vigente. La Declaración de Aplicabilidad (fila 110) confirma que la red está segmentada y que se controla el acceso de externos, aunque el reforzamiento de equipos con documentación estándar sigue en desarrollo y falta deshabilitar las conexiones de red sin uso. Se sugiere dejar en la brecha los aspectos puntuales que faltan para completar el control.
T.1.21	A 8.21	Seguridad de los servicios de red	80	La OTI sustenta el control únicamente con una referencia genérica a los lineamientos del manual de políticas de

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
				seguridad de la información sobre control de acceso de red y servicios en red. El numeral aplicable dentro del manual es el 4.18.5, Control de Acceso a la Red, que desarrolla lineamientos concretos sobre autenticación individual, cambio periódico de contraseñas privilegiadas, cifrado en transferencia de información clasificada, acceso de terceros bajo autorización de la OTI y segmentación por VLAN. El instrumento reporta una calificación de 80 sin indicar cuáles son los aspectos concretos que impiden alcanzar el cumplimiento total del control.
T.1.22	A 8.22	Segregación de redes	80	Conforme a lo reportado en el instrumento MSPI, la OTI sustenta este control en la segmentación de la red mediante VLAN sin precisar el código vigente del procedimiento en el sistema de gestión. Los numerales 4.18.5 (literal j.) y 4.28.1 del manual de políticas de seguridad de la información respaldan que la OTI debe mantener las redes segmentadas por VLANS, grupos de servicios y dependencias, así como definir mecanismos de separación basados en niveles de confianza. Sin embargo, no se encontró documentación que identifique cómo se clasifican las redes por nivel de confianza o importancia, ni cómo se tratan las redes inalámbricas de forma diferenciada respecto a las redes internas como exige el control. El instrumento reporta una calificación de 80 sin indicar qué aspectos específicos faltan para cumplir completamente con este control, por tanto, se sugiere registrar esta información en la actualización que se realice al instrumento.
T.1.23	A 8.23	Filtrado web	80	La OTI señala que hay políticas de navegación para prevenir la descarga de malware, sin citar el documento que las formaliza ni la plataforma que las aplica. Se identificó que la entidad opera una plataforma perimetral Fortinet, capaz de aplicar filtrado web, y que la hoja Cumplimiento v2022 (fila 94) del SOA 2025 y 2026 asigna 90 puntos a este control, cifra distinta a los 80 del instrumento, sin que ninguno de los documentos evidencie las categorías de sitios bloqueados ni la capacitación al personal sobre uso seguro de recursos en línea. Lo aconsejable es unificar la calificación y detallar en la brecha lo que falta para completar el control.
T.1.24	A 8.24	Uso de criptografía	80	Se reporta una política de llaves criptográficas con custodia en todo su ciclo de vida, pero sin citar el código del documento. El numeral 4.19 del manual pide determinar

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
				algoritmos autorizados, cambiar llaves cada año, administrar certificados digitales y revisar periódicamente las herramientas criptográficas; sin embargo, la Declaración de Aplicabilidad precisa que la OTI solo gestiona algunas llaves de tokens externos, certificados y firmas electrónicas, y los planes 2026 dejan pendientes la migración de protocolos de cifrado, la rotación de claves administrativas y la revisión de certificados. Por lo mencionado, falta relacionar en la brecha los aspectos, actividades o entregables que permitan cerrar el control.
T.1.25	A 8.25	Ciclo de vida de desarrollo seguro	60	La OTI indica que el manual define lineamientos de seguridad en desarrollo y soporte, sin precisar código ni numeral. Los numerales 4.29.2 y 4.29.3 del manual exigen definir principios de desarrollo seguro revisados cada año y aplicar los mismos controles de acceso en producción y desarrollo; no obstante, la Declaración de Aplicabilidad de ambas vigencias (fila 129) reconoce que los ambientes de desarrollo están en los portátiles de los desarrolladores, práctica que la propia entidad califica como inadecuada y que se mantiene igual entre 2025 y 2026. Se recomienda dejar en la brecha los aspectos pendientes para completar el control.
T.1.26	A 8.26	Requisitos de seguridad de la aplicación	80	La OTI reporta controles de acceso con credenciales, roles y privilegios, certificados en aplicativos web y hardening en Fiscaminero, sin citar el numeral que formaliza estos requisitos. El numeral 4.29.1 del manual solicita considerar el nivel de confianza en la autenticación, la protección de activos y el registro de eventos; además, la hoja Cumplimiento v2022 del SOA 2025 asigna 90 puntos frente a los 80 del instrumento, y en la revisión de aplicaciones de la intranet se encontró el aplicativo WebCenter Content con una URL marcada como "No segura" por el navegador. Por lo mencionado se considera importante revisar la calificación y precisar en la brecha lo que falta para cerrar el control.
T.1.27	A 8.27	Arquitectura del sistema seguro y principios de ingeniería	80	La OTI reporta que los principios de desarrollo seguro están definidos en el manual, sin citar el numeral aplicable. La Declaración de Aplicabilidad (fila 128) precisa que estos principios se encuentran en implementación, indicando una aplicación aún parcial y no consolidada, sin registros que acrediten su revisión periódica ni su aplicación en actividades concretas de ingeniería de sistemas. El

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
				instrumento reporta una calificación de 80 sin indicar qué aspectos específicos faltan para cumplir completamente con este control.
T.1.28	A 8.28	Codificación segura	60	La OTI no reporta información sobre cómo se cumple este control, dejando el campo de evidencia vacío. La Declaración de Aplicabilidad (fila 124) menciona que en el desarrollo de aplicaciones web se utilizan herramientas de seguridad, aunque sin detallar cuál es la práctica de codificación segura aplicada. El campo de brecha reconoce que se realizan actividades relacionadas, pero que estas deben documentarse, medirse y formalizarse. El instrumento reporta una calificación de 60 sin indicar qué aspectos específicos faltan para cumplir completamente con este control, por lo se sugiere adelantar las acciones necesarias para aumentar la calificación del control.
T.1.29	A 8.29	Pruebas de seguridad en desarrollo y aceptación	80	La respuesta reportada en el instrumento menciona los lineamientos de desarrollo seguro están en el manual, sin acreditar procedimientos ni registros de pruebas ejecutadas. Los numerales 4.29.5 y 4.29.6 exigen pruebas funcionales de seguridad, uso de herramientas de análisis y escáneres de vulnerabilidad, pruebas de aceptación por persona distinta de quien desarrolla y documentación de todo ello; sin embargo, no se hallaron registros de pruebas ni criterios de aceptación de seguridad formalizados antes del paso a producción. De acuerdo con lo expuesto, se recomienda registrar en el campo brecha los aspectos pendientes para completar el control.
T.1.30	A 8.30	Desarrollo subcontratado	80	La OTI respalda el control en los lineamientos de desarrollo seguro del manual, sin citar el numeral. El numeral 4.29.4 exige acuerdos de licenciamiento con derechos de propiedad intelectual, evidencia de pruebas de seguridad del desarrollador externo, pruebas de aceptación del software y el derecho de la ANM a auditar el desarrollo; la Declaración de Aplicabilidad (fila 130) solo confirma de forma general que el manual contempla los servicios tercerizados, sin registros de supervisión, evidencias de pruebas de terceros ni cláusulas de auditoría en los desarrollos recientes. Se recomienda precisar en la brecha lo que falta para cerrar el control.

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
T.1.31	A 8.31	Separación de los entornos de desarrollo, prueba y producción	60	La OTI describe protocolos de aceptación con pruebas de funcionalidad, estrés e integración, respuesta que no toca el objeto del control, que es separar los entornos de desarrollo, prueba y producción. La Declaración de Aplicabilidad (fila 129) reconoce que los ambientes de desarrollo están en los portátiles de los desarrolladores, práctica calificada como inadecuada, y hay inconsistencia en las calificaciones: 60 puntos en el instrumento frente a 80 en la hoja Cumplimiento v2022 (fila 103). Conviene unificar la calificación y registrar en la brecha los aspectos pendientes para completar el control.
T.1.32	A 8.32	Gestión de cambios	100	De acuerdo con lo reportado, la OTI cita un procedimiento de gestión de cambios (APO4-P-010), aunque en las anotaciones del instrumento se identifica que ese código ha sido actualizado a otro código diferente, lo que se suma a un hallazgo transversal de desactualización de códigos documentales. La Declaración de Aplicabilidad (filas 89, 125 y 126) confirma que existe procedimiento de gestión de cambios, herramienta asociada y pruebas previas antes de liberar sistemas. El instrumento reporta una calificación de 100 sin acreditar la vigencia del código citado ni aportar registros de cambios ejecutados que permitan verificar la aplicación del procedimiento. Se recomienda verificar la vigencia del código en el sistema integrado de gestión.
T.1.33	A 8.33	Información de prueba	80	La OTI reporta que se tiene establecido el no uso de datos reales en pruebas con lineamientos de confidencialidad para tal fin. Sin embargo, el propio instrumento anota que "*no se tiene*" autorización separada para copiar información operativa a un entorno de prueba, evidenciando una contradicción. Esta contradicción se confirma en la Declaración de Aplicabilidad (fila 134), que reconoce que actualmente se utilizan datos de producción para pruebas y no existen procedimientos apropiados para protegerlos. El numeral 4.29.7 del manual de políticas de seguridad de la información establece que la información entregada para pruebas debe estar enmascarada y los datos sensibles eliminados, conforme a la Ley de Protección de Datos

ID. ITEM	CONTROL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	OBSERVACIONES OCI
				Personales. El instrumento reporta una calificación de 80 sin acreditar el cumplimiento de estos requisitos.
T.1.34	A 8.34	Protección de los sistemas de información durante las pruebas de auditoría	80	La evidencia aportada corresponde a lineamientos de desarrollo seguro, que no atienden el objeto del control: planificar y proteger las pruebas de auditoría técnica. El numeral 4.27.1 pide acordar los requisitos de auditoría, controlar el alcance de las pruebas técnicas, ejecutarlas en horario controlado, registrar accesos y logs y limitarlas a acceso de lectura; el instrumento menciona "Acuerdos técnicos de entendimiento" y registros de logs, pero la OTI no aportó esos documentos. Se sugiere precisar en la brecha los aspectos pendientes para completar el control.

Fuente: Matriz de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), diligenciada por la Oficina de Tecnologías de la Información (OTI) - 2026.

6.7. Evaluación bajo el Marco de Ciberseguridad NIST (Cybersecurity Framework):

Como complemento a la evaluación de los controles del Anexo A de la norma NTC-ISO/IEC 27001:2022, el instrumento de autodiagnóstico incorpora una valoración de la entidad frente al Marco de Ciberseguridad NIST (Cybersecurity Framework), estructurado en seis funciones: Gobernar (GV), Identificar (ID), Proteger (PR), Detectar (DE), Responder (RS) y Recuperar (RC). A diferencia de una evaluación autónoma, este componente no se diligencia de forma independiente, sino que cada categoría del marco NIST toma su calificación a partir de las cláusulas y controles ISO 27001 con los que se encuentra relacionada, de manera que sus resultados reflejan y consolidan lo ya valorado en los dominios del modelo.

Debido a lo anterior, la validación de la Oficina de Control Interno se orientó a verificar la consistencia entre la calificación asignada a cada categoría del marco NIST y la calificación de las cláusulas o controles ISO 27001 que le sirven de fuente, identificando si el resultado coincide o presenta diferencia.

El detalle del cotejo se presenta en la Tabla 6:

Tabla 6 Elementos asociados a NIST

Función	Categoría (Identificador)	Calif. NIST	Cláusula / Control ISO 27001 asociado	Calif. ISO	Resultado del cotejo
Gobernar (GV)	Contexto organizativo (GV.OC)	**70**	4. Contexto de la organización	**70**	Coincide
Gobernar (GV)	Estrategia de gestión de riesgos (GV.RM)	**0**	6.1 Acciones para tratar los riesgos y oportunidades	**0**	Coincide
Gobernar (GV)	Funciones, responsabilidades y autoridades (GV.RR)	**86,7**	5.2 Funciones y responsabilidades; 5.3 Segregación de funciones; 5.5 Contacto con las autoridades	**86,7**	Coincide
Gobernar (GV)	Política (GV.PO)	**100**	5.1 Políticas de seguridad; 5.2 Política	**100**	Coincide
Gobernar (GV)	Supervisión (GV.OV)	**80**	8.16 Actividades de supervisión	**80**	Coincide
Gobernar (GV)	Gestión de riesgos de la cadena de suministro (GV.SC)	**80**	5.21 Seguridad en la cadena de suministro TIC	**80**	Coincide
Identificar (ID)	Gestión de activos (ID.AM)	**80**	5.9 Inventario; 5.10 Uso aceptable; 5.11 Devolución de activos	**80**	Coincide
Identificar (ID)	Evaluación de riesgos (ID.RA)	**100**	8.2 Evaluación de riesgos de seguridad de la información	**100**	Coincide
Identificar (ID)	Mejora (ID.IM)	**100**	10.1 Mejora continua; 10.2 No conformidad y acciones correctivas	**100**	Coincide
Proteger (PR)	Gestión de identidades, autenticación y control de acceso (PR.AA)	**70**	8.2, 8.3, 8.4, 8.5, 5.15, 5.16, 5.17, 5.18 (control de acceso)	**82,5**	**Diferencia**
Proteger (PR)	Concienciación y capacitación (PR.AT)	**100**	6.3 Concientización, educación y capacitación	**100**	Coincide
Proteger (PR)	Seguridad de datos (PR.DS)	**70**	8.11 Enmascaramiento de datos; 8.12 Prevención de fuga de datos	**70**	Coincide
Proteger (PR)	Seguridad de plataformas (PR.PS)	**80**	8.21 Seguridad de los servicios de red	**80**	Coincide
Proteger (PR)	Resistencia de la infraestructura tecnológica (PR.IR)	**80**	8.27 Arquitectura del sistema seguro y principios de ingeniería	**80**	Coincide
Detectar (DE)	Monitoreo continuo (DE.CM)	**80**	9.1 Seguimiento, medición, análisis y evaluación	**80**	Coincide
Detectar (DE)	Análisis de eventos adversos (DE.AE)	**80**	5.25 Evaluación y decisión sobre eventos de seguridad	**80**	Coincide
Responder (RS)	Gestión de incidentes (RS.MA)	**100**	5.24 Planificación y preparación de la gestión de incidentes	**100**	Coincide
Responder (RS)	Análisis de incidentes (RS.AN)	**100**	5.24 Planificación y preparación de la gestión de incidentes	**100**	Coincide

Función	Categoría (Identificador)	Calif. NIST	Cláusula / Control ISO 27001 asociado	Calif. ISO	Resultado del cotejo
Responder (RS)	Notificación y comunicación de la respuesta (RS.CO)	**100**	5.26 Respuesta a incidentes de seguridad de la información	**100**	Coincide
Responder (RS)	Mitigación de incidentes (RS.MI)	**100**	5.26 Respuesta a incidentes de seguridad de la información	**100**	Coincide
Recuperar (RC)	Ejecución del plan de recuperación (RC.RP)	**100**	5.24 Planificación y preparación de la gestión de incidentes	**100**	Coincide
Recuperar (RC)	Comunicación de la recuperación (RC.CO)	**100**	5.26 Respuesta a incidentes de seguridad de la información	**100**	Coincide
PROMEDIO FRAMEWORK NIST		**84,4**			

Fuente: Matriz de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), diligenciada por la Oficina de Tecnologías de la Información (OTI) - 2026.

Derivado de lo anterior, la única diferencia se observó en la categoría Gestión de identidades, autenticación y control de acceso (PR.AA), la cual registra una calificación de 70 frente a un promedio de 82,5 de los controles de acceso que la componen, situación atribuible a que su valoración se ancló en los controles de acceso de menor puntaje del dominio y no en el promedio del conjunto.

En consecuencia, el resultado del componente NIST, con un promedio de 84,4 sobre 100, es consistente con el nivel de madurez global reportado en la evaluación de controles del Anexo A.

6.8. Planificación:

El Documento Maestro indica: "*Para el desarrollo de esta fase se deben utilizar los resultados de la fase anterior y proceder a elaborar el Plan de Seguridad y Privacidad de la Información, con el objetivo de que la entidad realice la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI*". Para el cumplimiento de esta fase, el Documento Maestro establece un conjunto de documentos que la entidad debe generar. En atención a ello, se cotejó cada uno de los entregables exigidos frente a la documentación aportada por la dependencia, obteniendo el siguiente resultado:

- √ **Alcance MSPI:** cubierto en el numeral 2 del Manual de Políticas de Seguridad de la Información APO4-M-002 V2, complementado con la Política General del numeral 4.2.

√ **Acto administrativo con las funciones de seguridad y privacidad de la información:** no aportado; su expedición se encuentra pendiente según lo tratado sesión de Comité Institucional de Gestión y Desempeño.

√ **Adopción de la Política de Seguridad mediante acto administrativo:** la Política fue aprobada por la Presidencia de la ANM al interior del Manual APO4-M-002 V2 (10/Dic/2024).

√ **Documento de roles y responsabilidades:** cubierto en el numeral 4.4 del Manual de políticas de seguridad de la información APO4-M-002 V2, que desarrolla los roles de la Alta Dirección, el Comité Institucional de Gestión y Desempeño, la OTI, el Oficial de Seguridad y el propietario del activo.

De manera complementaria, conforme al numeral 7.2.3 del documento maestro Guía de Implementación del MSPI, se observa que la figura de Oficial de Seguridad se ejerce actualmente dentro de la OTI, situación que no resulta coherente con la dependencia de un área estratégica distinta a la de Tecnología exigida por dicho lineamiento, el cual dispone además su integración con voz y voto al Comité Institucional de Gestión y Desempeño y con voz, sin voto, al Comité de Control Interno. Se recomienda a la entidad valorar la pertinencia de ajustar esta dependencia conforme al documento maestro.

√ **Procedimiento de inventario y clasificación de la información e infraestructura crítica:** el Manual APO4-M-002 V2 lo refiere con el código APO4-P-009, el cual no se encuentra vigente en Isolucion, correspondiendo el actual a Gestión de Activos de Información código TI-P-003, versión 1, del 21 de octubre de 2025. El entregable queda cubierto mediante el procedimiento vigente TI-P-003 y el inventario de activos en formato MSPI aunque persiste la desactualización de la referencia en el manual. Se recomienda actualizar dicha referencia al código vigente TI-P-003 y verificar que las demás remisiones documentales correspondan a las versiones actuales del sistema.

√ **Metodología de inventario y clasificación:** cubierta mediante la Matriz de Clasificación de Activos de Información, versión 2, con corte a diciembre de 2025, instrumento en el que la entidad define los criterios de valoración de confidencialidad, integridad y disponibilidad y los niveles de clasificación aplicados a los activos. Este documento se articula con el procedimiento vigente de Gestión de Activos de Información TI-P-003 y con el inventario en formato MSPI, dando cuenta de la metodología exigida para la fase.

- √ **Política de Gestión de Riesgos y sus lineamientos:** se encuentra cubierta mediante la Política para la Gestión Integral del Riesgo en la ANM, en su versión 2 de la vigencia 2026, la cual actualiza la Política de Administración de Riesgos de 2021 y se articula con el numeral 4.32 del Manual APO4-M-002 V2. Esta política aborda de manera expresa los riesgos de seguridad de la información y ciberseguridad, con criterios de valoración sobre confidencialidad, integridad y disponibilidad y niveles de aceptación diferenciados según la zona de riesgo residual, con lo cual el entregable exigido para la fase se encuentra cubierto. No obstante, no fue posible identificar dicha política publicada dentro de Isolucion, por lo que se recomienda verificar su cargue y oficialización en dicha herramienta.

- √ **Plan de tratamiento de riesgos:** la entidad cuenta con el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026, formalizado por el Oficial de Seguridad de la Información con fecha del 29 de diciembre de 2025, el cual desarrolla la metodología bajo el ciclo PHVA, las fases de tratamiento y la evolución trimestral de los riesgos de la vigencia 2025, dando cumplimiento al entregable exigido para la fase.

- √ **Declaración de aplicabilidad:** la entidad dispone de la Declaración de Aplicabilidad (SOA) correspondiente a las vigencias 2025 y 2026. No obstante, la hoja que formaliza la declaración de aplicabilidad control por control, con su justificación de aplicabilidad, se encuentra estructurada sobre los dominios y controles de la versión ISO/IEC 27001:2013. Si bien el mismo archivo incorpora una hoja de cumplimiento que mapea los controles del Anexo A de la NTC-ISO/IEC 27001:2022, la Declaración de Aplicabilidad como tal aún no fue migrada a la estructura de la versión 2022, en concordancia con el hallazgo transversal sobre la operación del sistema de gestión bajo la versión 2013 de la norma. Se recomienda formalizar la Declaración de Aplicabilidad conforme a la NTC-ISO/IEC 27001:2022 adoptada por la Resolución 02277 de 2025.

- √ **Manual de políticas de seguridad de la información:** la entidad cuenta con el Manual de Políticas de Seguridad de la Información APO4-M-002, versión 2, vigente desde el 10 de diciembre de 2024 y aprobado por la Presidencia de la ANM, el cual desarrolla el objetivo, alcance, roles y lineamientos de seguridad de la información.

- √ **Plan de Cambio, Cultura y Apropiación:** la entidad dispone del Plan de Socialización SI-TIC ANM correspondiente a la vigencia 2026, que programa las actividades de socialización, sensibilización y apropiación en seguridad

de la información dirigidas a los colaboradores, dando cumplimiento al entregable exigido para la fase.

6.9. Operación:

Para esta fase el documento maestro MSPI indica: "*Tras finalizar la fase 7 de planeación del MSPI, se iniciará la implementación de los procesos de seguridad de la información: gestión de activos, riesgos, incidentes, vulnerabilidades, tratamiento y evaluación de controles. Se fomentará la cultura de seguridad y se definirán criterios de cumplimiento y mecanismos de control para procesos y servicios externos relevantes, asegurando su alineación con el SGSI*."

En el marco del seguimiento al Modelo de Seguridad y Privacidad de la Información (MSPI), la Oficina de Control Interno realiza la validación correspondiente a la Fase 2 – Operación, la cual contempla la implementación de los procesos de seguridad de la información relacionados con la gestión de activos, riesgos, incidentes, vulnerabilidades, tratamiento y evaluación de controles.

Durante esta fase, la OCI verificó la existencia, actualización y aplicación de los documentos exigidos, tales como el inventario de información, la matriz de riesgos, el plan de implementación de controles, la gestión de eventos e incidentes, la gestión de vulnerabilidades y la evidencia de la implementación de los controles de seguridad de la información, con el propósito de constatar el avance del MSPI y su alineación con el Sistema de Gestión de Seguridad de la Información (SGSI).

El instrumento MSPI indica que se deben generar los siguientes documentos:

- **Actualización del inventario de información.** Durante la vigencia 2025 la entidad actualizó el inventario de activos de información en formato MSPI, con registros clasificados de acuerdo con su procedimiento de Gestión de Activos de Información, acompañado de la matriz de clasificación de activos.
- **Actualización de la matriz de riesgos de seguridad de la información**. Se evidencia la matriz de riesgos de seguridad de la información y ciberseguridad con corte al cuarto trimestre de 2025, en la cual se identifican y valoran los riesgos sobre los pilares de confidencialidad, integridad y disponibilidad, con seguimiento a su evolución a lo largo de la vigencia.

- **Plan de implementación de controles de seguridad.** La OTI remite el plan de implementación de controles para la vigencia, el cual detalla, entre otros campos, los riesgos, el tipo de riesgo, la naturaleza del control, la actividad específica, el control asociado a la NTC-ISO/IEC 27001:2022, los responsables, las fechas de inicio y finalización y la evidencia.
- **Actualización de la gestión de eventos e incidentes de seguridad de la información.** Se constata el registro y administración de los eventos e incidentes de seguridad de la información a través de las herramientas de mesa de ayuda de la Oficina de Tecnología e Información, con la trazabilidad de los casos reportados, su análisis y tratamiento durante la vigencia 2025.
- **Actualización de la gestión de vulnerabilidades.** Se evidencian los documentos técnicos elaborados por la Oficina de Tecnología e Información que registran los resultados de las pruebas de vulnerabilidad sobre las aplicaciones y la infraestructura de la entidad, con sus respectivos retest y acciones de remediación.
- **Evidencia de la implementación de los controles de seguridad de la información.** Se identifican avances en la implementación de los controles del Anexo A de acuerdo con los resultados del instrumento de evaluación del MSPI, cuyo análisis control por control se desarrolla en el numeral 6.3 del presente informe. Algunos controles se encuentran implementados, mientras otros permanecen en fase de fortalecimiento.

Posteriormente, el instrumento MSPI para esta fase se subdivide en 3 elementos, como se detalla en la Tabla 7:

Tabla 7 Elementos asociados a la fase de Operación – Observaciones de la Oficina de Control Interno.

NUM	DESCRIPCIÓN	REQUISITOS	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	Seguimiento OCI
8.1	Planificación y control operacional	Planificar, implementar, controlar y documentar el proceso del SGSI para gestionar los	**80**	El proceso reporta una calificación de 80 en el instrumento MSPI. Como evidencia se relacionan los procesos documentados para la operación del SGSI y el uso de la herramienta de gestión documental Isolucion como repositorio de los recursos. El propio

NUM	DESCRIPCIÓN	REQUISITOS	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	Seguimiento OCI
		riesgos (i.e. un plan de tratamiento de riesgos)		instrumento señala como aspecto por fortalecer que los procesos se diseñen conforme a las necesidades del negocio bajo el enfoque de seguridad desde el diseño, guardando relación con los lineamientos de gestión y calidad documental de la entidad, y que la organización mantenga pleno conocimiento y control de los procesos, productos y servicios prestados por terceros relevantes para el SGSI. En consecuencia, se recomienda diligenciar el campo de brecha relacionando estos aspectos pendientes para alcanzar el cumplimiento total del control.
8.2	Evaluación de riesgos de seguridad de la información	(Re)hacer la apreciación y documentar los riesgos de seguridad de la información en forma regular y ante cambios o modificaciones	**100**	Este componente registra una calificación de 100 en el instrumento MSPI; sin embargo, como evidencia no se aporta un soporte directo, sino que se remite al numeral 6.1 del mismo instrumento. Al verificar dicha remisión se identifica que el numeral 6.1, relativo a las acciones para tratar los riesgos y que corresponde a la planificación del mismo proceso de apreciación de riesgos, se encuentra calificado en cero, lo que resulta contradictorio con la calificación máxima asignada a su evaluación en la operación. En consecuencia, la evidencia aportada por remisión no respalda de manera directa el cumplimiento del requisito, por lo que se recomienda revalidar la calificación otorgada, precisar en el instrumento la evidencia documental específica que sustente la apreciación periódica de

NUM	DESCRIPCIÓN	REQUISITOS	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	Seguimiento OCI
				los riesgos y asegurar la coherencia con la calificación del numeral mencionado.
8.3	Tratamiento del riesgo de seguridad de la información	Implementar el plan de tratamiento de riesgos (tratar los riesgos) y documentar los resultados	**100**	El proceso presenta una calificación de 100 en el instrumento MSPI, relacionando como evidencia el plan de seguridad de la información constituido a partir de los resultados de la gestión de riesgos. El propio instrumento señala como aspecto por fortalecer el establecimiento de las medidas de tratamiento en el marco de un plan que sirva de insumo detallado para el plan de seguridad de la información, así como la realización de pruebas de diseño y efectividad sobre las medidas de control implementadas, con el fin de comprobar que los controles estén tratando el riesgo conforme a lo concebido. Adicionalmente, se advierte una inconsistencia en las calificaciones del instrumento, toda vez que este requisito de tratamiento del riesgo se califica en 100, mientras que la cláusula 6.1, relativa a las acciones para tratar los riesgos y oportunidades y que constituye su fase de planificación, registra un puntaje de cero. Se recomienda revalidar la coherencia entre ambas calificaciones e incorporar las pruebas de efectividad como soporte de la operación del control.

Fuente: Matriz de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), diligenciada por la Oficina de Tecnologías de la Información (OTI) - 2026.

El promedio del componente de Operación en el instrumento es de 93 sobre 100, lo que ubica esta fase entre las de mayor avance del modelo.

No obstante, el análisis anterior evidencia que dicho promedio se sustenta en calificaciones que, en los requisitos 8.2 y 8.3, no cuentan con evidencia directa suficiente o presentan inconsistencias frente a otras cláusulas del instrumento, por lo que se recomienda revalidar los soportes que respaldan la puntuación asignada.

6.10. Evaluación del desempeño:

Para validación de la fase de evaluación del desempeño del Modelo de Seguridad y Privacidad de la Información, se enfoca en verificar la efectividad de las acciones implementadas durante la fase de operación, mediante el análisis de los indicadores definidos en la etapa de implementación.

Una vez culminadas las actividades correspondientes a la fase de operación del Modelo de Seguridad y Privacidad de la Información (MSPI), la Oficina de Control Interno realizó la evaluación de la efectividad de las acciones implementadas, tomando como referencia los indicadores definidos en la fase de implementación.

Este seguimiento buscó verificar la adecuada interacción entre el MSPI, el Modelo Integrado de Planeación y Gestión (MIPG) y el cumplimiento de los requerimientos establecidos en la Ley 1581 de 2012 sobre protección de datos personales, la Ley 1712 de 2014 de transparencia y acceso a la información pública, así como las demás disposiciones normativas que las reglamenten, adicionen, modifiquen o deroguen.

Los elementos que componen esta fase se relacionan en la Tabla 8:

Tabla 8 Elementos asociados a la fase de Evaluación del desempeño – Observaciones de la Oficina de Control Interno.

Numeral	Descripción	Calificación OTI ANEXO A ISO 27001	Seguimiento OCI
9.1	Seguimiento, medición,	**80**	El proceso registra una calificación de 80 en el instrumento MSPI. Como evidencia se relaciona el monitoreo al sistema de gestión de seguridad y a los

Numeral	Descripción	Calificación OTI ANEXO A ISO 27001	Seguimiento OCI
	análisis y evaluación		riesgos a través de la matriz de riesgos, del cual se deriva un informe de gestión. No obstante, el propio instrumento señala que el proceso de seguimiento y medición no se encuentra conducido por unos lineamientos que definan la metodología del monitoreo, su periodicidad, los responsables de ejecutarlo y de analizar los resultados obtenidos. En consecuencia, se recomienda diligenciar el campo de brecha relacionando dichos aspectos y formalizar los lineamientos de seguimiento y medición del SGSI, con el fin de alcanzar el cumplimiento total del requisito.
9.2	Auditoría interna	**80**	El componente reporta una calificación de 80 en el instrumento MSPI. Como evidencia la entidad relaciona la evaluación realizada al sistema por parte del gobierno nacional, conocida en reunión con los encargados de la administración del SGSI, sin que dentro de la documentación aportada se haya allegado el soporte de dicha evaluación. Sobre el particular se precisa que el requisito exige planificar y llevar a cabo auditorías internas del SGSI, ejercicio que corresponde a la Oficina de Control Interno y que difiere de una evaluación externa. Al respecto, se aclara que para la vigencia 2025, y como limitante de auditoría, la Oficina de Control Interno adelantó seguimiento a aspectos de seguridad de la información, sin que hubiese sido posible ejecutar una auditoría específica al Modelo de Seguridad y Privacidad de la Información; ejercicio que precisamente se está desarrollando en la vigencia 2026 a través de la presente auditoría. En consecuencia, se recomienda soportar en el instrumento las auditorías internas efectivamente ejecutadas al MSPI, actualizar dicha evidencia una vez culmine el presente ejercicio y diligenciar el campo de brecha con los aspectos pendientes para alcanzar el cumplimiento total del control.
9.3	Revisión por la dirección	**100**	El proceso presenta una calificación de 100 en el instrumento MSPI. Como evidencia se relaciona que la evaluación realizada al sistema por parte del gobierno nacional fue de conocimiento de los encargados de la administración del SGSI y de la alta dirección, según lo

Numeral	Descripción	Calificación OTI ANEXO A ISO 27001	Seguimiento OCI
			observado en reunión. No obstante, dicha evidencia se soporta en una manifestación verbal y no en un registro documental que acredite formalmente la revisión por la dirección del SGSI, entendida como el ejercicio en el cual la alta dirección revisa los resultados del desempeño, los objetivos y la eficacia del sistema para la toma de decisiones. El propio instrumento recomienda conservar las evidencias en medio comprobable, tales como actas, correos o reuniones, que permitan establecer las decisiones adoptadas. En consecuencia, se sugiere revalidar la calificación otorgada y soportar la revisión por la dirección mediante los registros formales correspondientes.

Fuente: Matriz de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), diligenciada por la Oficina de Tecnologías de la Información (OTI) - 2026.

El componente de Evaluación del Desempeño alcanza un promedio de 87 sobre 100 en el instrumento; no obstante, para los tres requisitos las evidencias corresponden a manifestaciones verbales o referencias generales sin respaldo documental que acredite la formalización de los lineamientos de seguimiento, la ejecución de auditorías internas al SGSI y la revisión por la dirección, por lo que se recomienda revalidar las calificaciones y fortalecer los soportes que las sustentan.

6.11. Mejoramiento continuo:

En esta fase la Oficina de Control Interno valida las actividades adelantadas respecto al mejoramiento continuo de la seguridad y privacidad de la información, el cual hace parte del Modelo de Seguridad y Privacidad de la Información (MSPI) y tiene por objeto asegurar que las debilidades, hallazgos y oportunidades de mejora identificadas se traduzcan en acciones que fortalezcan de manera sostenida el Sistema de Gestión de Seguridad de la Información (SGSI).

Los elementos que componen esta fase se relacionan en la Tabla 9:

Tabla 9 Elementos asociados a la fase de Mejoramiento continuo – Observaciones de la Oficina de Control Interno.

Numeral	Descripción	Nivel de cumplimiento ANEXO A ISO 27001	Seguimiento OCI
10.1	Mejora continua	**100**	El proceso presenta una calificación de 100 en el instrumento MSPI. Como evidencia se relaciona que las acciones orientadas a detectar situaciones que demandan mejora y tratamiento del riesgo se consolidan como parte del Plan de Seguridad de la Información. Si bien la calificación es la máxima, la evidencia no se acompaña de un registro documental que dé cuenta del ciclo de mejora continua aplicado sobre el SGSI. En consecuencia, y en línea con la recomendación planteada en el propio instrumento, se recomienda generar y conservar una base de información que registre los hallazgos, oportunidades de mejora y observaciones, junto con las acciones adoptadas para su subsanación, de manera que estas evidencias soporten la aplicación del ciclo de mejora continua sobre el SGSI y permitan revalidar la calificación otorgada.
10.2	No conformidad y acciones correctivas	**100**	Este componente obtiene una calificación de 100 en el instrumento MSPI. Como evidencia se relaciona la gestión del Plan de Seguridad de la Información a partir de las debilidades y riesgos materializados durante la operación. No obstante, la evidencia no acredita la identificación, análisis y tratamiento formal de no conformidades de seguridad de la información, ni el registro de las acciones correctivas adoptadas para prevenir su recurrencia, conforme lo exige el requisito; asimismo, no se evidencian planes de mejoramiento oficializados en el sistema Isolucion asociados a esta materia. En consecuencia, y en línea con la recomendación planteada en el propio instrumento, se sugiere contar con informes periódicos de cierre que sirvan de insumo para la consolidación del plan estratégico de seguridad de la información, así como formalizar en Isolucion los planes de mejoramiento y referenciar los documentos que soporten el registro

Numeral	Descripción	Nivel de cumplimiento ANEXO A ISO 27001	Seguimiento OCI
			y la trazabilidad de las no conformidades y acciones correctivas del SGSI, de manera que se pueda revalidar la calificación otorgada.

Fuente: Matriz de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), diligenciada por la Oficina de Tecnologías de la Información (OTI) - 2026.

El componente de Mejora Continua alcanza un promedio de 100 sobre 100 en el instrumento. No obstante, el análisis evidencia que dicha calificación se soporta en la remisión general al Plan de Seguridad de la Información, sin el respaldo documental que acredite el registro de hallazgos, no conformidades y acciones correctivas propias del ciclo de mejora continua, por lo que se recomienda revalidar las calificaciones y consolidar las evidencias que las sustentan.

Una vez culminada la revisión del instrumento MSPI se presenta la siguiente oportunidad de mejora:

Oportunidad de Mejora No. 2: Debilidades en el diligenciamiento, soporte y coherencia interna del instrumento de autodiagnóstico MSPI.

Se identifica por parte del equipo auditor que el instrumento de autodiagnóstico presenta las siguientes situaciones:

- El campo de brecha no fue diligenciado en ninguno de los 93 controles del Anexo A evaluados, pese a que 65 registran calificación inferior a la meta de 100.

- En la sección cláusulas del instrumento, solo 4 de los 23 numerales evaluados cuentan con brecha registrada, quedando 9 numerales con calificación inferior a la meta sin este campo.

- El requisito 8.2, evaluación de riesgos de seguridad de la información, se califica con 100 y registra como única evidencia la anotación "Se tienen las evidencias conforme al punto 6.1.5", referencia que no corresponde a ningún numeral del instrumento.

- Los requisitos 9.2, auditoría interna, y 9.3, revisión por la dirección, sustentan su evidencia en lo observado en reunión, sin acta, informe o programa que acredite las actividades.

- Los requisitos 10.1 y 10.2 registran calificación de 100 y, a la vez, solicitan en su campo de recomendación constituir la base de registro de hallazgos y el informe de cierre que darían soporte a esa calificación.

- En el componente NIST, la categoría PR.AA registra 70 frente a un promedio de 82,5 de los ocho controles del Anexo A que la alimentan.

Lo anterior expone a la entidad a que el nivel de madurez reportado no corresponda al estado real del modelo ni resulte verificable por un tercero, de manera que las brechas no registradas permanezcan sin tratamiento, la planificación de la siguiente vigencia se estructure sobre una línea base no confiable y la información remitida a las instancias de control carezca del respaldo documental que la sustente.

Recomendación:

Se sugiere a la Oficina de Tecnologías e Información revalidar el diligenciamiento del instrumento de autodiagnóstico MSPI, de manera que cada calificación cuente con la evidencia documental que la respalda y que se registre la brecha en los controles y numerales que no alcanzan la meta, asegurando además la consistencia entre las hojas e información del instrumento.

Lo anterior en atención a que la fase de diagnóstico constituye la línea base de las fases posteriores del modelo, por lo que su diligenciamiento completo condiciona la confiabilidad de la planificación asociada al tema.

6.12. Validación SIG - Isolucion:

De manera transversal al desarrollo de la auditoría, el equipo auditor validó el Sistema Integrado de Gestión (SIG), contrastando la documentación registrada en el aplicativo Isolucion frente al Mapa de Procesos oficial de la Agencia.

De este ejercicio se identifica una diferencia en la denominación de los procesos bajo los cuales se encuentra clasificada la documentación relacionada con la seguridad de la información, así:

Imagen 5 Mapa de Procesos institucional – Agencia Nacional de Minería.

Fuente:

Mapa de Procesos institucional, Sistema Integrado de Gestión (SIG) – Agencia Nacional de Minería.

Como se observa en la Imagen 5, el Mapa de Procesos institucional contiene dos procesos relacionados con la gestión tecnológica: uno de naturaleza estratégica, denominado "Estrategia y Gobierno de TIC", y uno de apoyo, denominado "Gestión de Tecnologías e Información".

Ahora bien, en la Imagen 6 se evidencia que, en términos generales, la documentación consultada en Isolucion sí se encuentra asociada correctamente a estos dos procesos, identificados con los códigos EG-P-003 y TI-P-010, respectivamente.

Imagen 6 Documentos asociados a los procesos "Estrategia y Gobierno de TIC" y "Gestión de Tecnologías e Información" en Isolucion.

Fuente: *Aplicativo Isolucion – Agencia Nacional de Minería. Captura de pantalla tomada por el equipo auditor.*

No obstante, en la Imagen 7 se identificó que el documento "Políticas de Seguridad de la Información" (código APO4-M-002) se encuentra clasificado en Isolucion bajo un tercer proceso, denominado "Administración de Tecnologías e Información", que no corresponden a ninguno de los dos procesos actualmente vigentes en el Mapa de Procesos institucional.

Imagen 7 Documento "Políticas de Seguridad de la Información" (APO4-M-002) asociado a un proceso no vigente en Isolucion.

Fuente: *Aplicativo Isolucion – Agencia Nacional de Minería. Captura de pantalla tomada por el equipo auditor.*

Por lo descrito se presenta la siguiente oportunidad de mejora:

Oportunidad de Mejora No. 3: Falta de alineación entre el Mapa de Procesos institucional y la clasificación documental registrada en el aplicativo Isolucion.

Con lo mencionado se identifica que el aplicativo Isolucion conserva documentación clasificada bajo una denominación de proceso que no se encuentra vigente en el Mapa de Procesos institucional, situación que recae sobre el documento que soporta la política de seguridad de la información de la entidad y que constituye fuente de evidencia de varios de los controles evaluados en el presente informe.

Lo anterior genera riesgo de confusión para los usuarios del Sistema Integrado de Gestión al momento de ubicar o consultar la documentación aplicable, afecta la trazabilidad entre la estructura de procesos vigente y sus documentos asociados,

y puede derivar en la coexistencia de codificaciones documentales inconsistentes dentro del mismo dominio de gestión tecnológica.

Ahora bien, mediante correo electrónico remitido por la OTI aportó al equipo auditor el documento Políticas de Seguridad de la Información, el cual se encuentra en proceso de actualización y será presentado al Comité Institucional de Gestión y Desempeño programado para el 8 de septiembre de 2026, cuya agenda contempla un punto específico para la aprobación de los documentos relacionados con seguridad de la información, entre ellos la política.

La dependencia menciona que esta actualización se viene adelantando desde hace aproximadamente 6 meses y que concluye con la aprobación en el comité.

Una vez surtida dicha aprobación, el Grupo de Planeación asignará el código correspondiente conforme al proceso vigente en el Mapa de Procesos institucional y se procederá con su publicación en el aplicativo Isolucion

Recomendación:

Se sugiere al Grupo de Planeación, en articulación con la OTI, realizar la revisión y depuración de la totalidad de los documentos registrados en Isolucion y asociados a la gestión tecnológica de la entidad, en concordancia con el Mapa de Procesos.

En atención a que la acción se encuentra en curso y su culminación depende de la sesión del Comité Institucional de Gestión y Desempeño programada para el 8 de septiembre de 2026, la presente oportunidad de mejora no requiere la formulación de un plan de mejoramiento ni su registro en el aplicativo Isolucion.

No obstante, el asunto queda sujeto a monitoreo por parte de la OCI, el cual se realizará el día 30 de septiembre de 2026 y, en caso de que una vez surtida la sesión del comité los documentos no se encuentren actualizados, codificados y publicados conforme al Mapa de Procesos vigente, se procederá con el registro en la plataforma para que el proceso responsable formule el plan de mejoramiento.

7. CONCLUSIONES

Se observa que la Agencia Nacional de Minería cuenta con una base institucional sólida para la operación del Modelo de Seguridad y Privacidad de la Información, reflejada en la existencia de una política de seguridad formalizada, un inventario

de activos clasificado, la gestión de riesgos, el seguimiento de eventos e incidentes de seguridad y el tratamiento de vulnerabilidades en los sistemas de información.

La Oficina de Tecnología e Información ha mantenido un compromiso constante con la implementación y continuidad del modelo, evidenciado en la documentación aportada y en el avance registrado a lo largo de las fases evaluadas.

No obstante, se identificaron aspectos que requieren atención prioritaria, principalmente relacionados con el diligenciamiento del instrumento de autodiagnóstico del MSPI y la consolidación y el levantamiento de las evidencias que sustentan las calificaciones asignadas, situaciones que apuntan a la trazabilidad, la verificación objetiva del cumplimiento y la medición del nivel de madurez del modelo.

A ello se suma la necesidad de actualizar la documentación del sistema de gestión frente a la versión vigente de la norma NTC-ISO/IEC 27001:2022 y de surtir la adopción formal del modelo mediante los actos administrativos correspondientes, aspectos que representan riesgos para la evaluación integral del desempeño institucional en materia de seguridad y privacidad de la información.

De igual manera, la validación transversal a las herramientas del SIG evidenció que el aplicativo Isolucion conserva documentación clasificada bajo una denominación de proceso no vigente en el Mapa de Procesos, situación que recae sobre el documento que soporta la política de seguridad de la información.

Su depuración permitirá asegurar la trazabilidad entre la estructura de procesos de la entidad y la documentación que sustenta el modelo. La entidad informó que la actualización de dicho documento se encuentra en curso y será sometida a consideración del Comité Institucional de Gestión y Desempeño, por lo que el asunto queda sujeto a monitoreo por parte de la Oficina de Control Interno, el 30 de septiembre de los corrientes.

Finalmente, aunque los resultados obtenidos reflejan la necesidad de continuar con el fortalecimiento del modelo, se reconoce el avance institucional en la gestión técnica y documental, así como la voluntad de mejora continua.

La implementación de las recomendaciones propuestas contribuirá al incremento del nivel de madurez del MSPI, al cumplimiento del marco normativo vigente y al aseguramiento progresivo de los principios de confidencialidad, integridad y disponibilidad de la información institucional.

8. RECOMENDACIONES

- ✓Adoptar las acciones necesarias para completar el levantamiento de los 42 ítems del instrumento MSPI, con evidencias actualizadas y verificables, priorizando los aspectos pendientes de acreditación, en particular la autoevaluación, la estratificación de la entidad y los inventarios de áreas de procesamiento y de terceros.

- ✓Diligenciar de manera completa el instrumento MSPI, incluido el campo de brechas, y establecer un mecanismo de revisión periódica que permita medir el grado de avance del modelo y garantizar la coherencia entre la información registrada y el estado real de su implementación.

- ✓Actualizar la documentación del Sistema de Gestión de Seguridad de la Información conforme a la versión vigente de la norma NTC-ISO/IEC 27001:2022, adoptada mediante la Resolución 02277 de 2025.

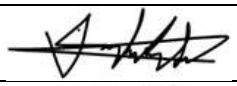
- ✓Fortalecer la gestión documental y de evidencias del MSPI, implementando una estructura organizada y estandarizada del repositorio institucional que permita la fácil identificación, acceso y trazabilidad de los documentos conforme a los numerales y componentes definidos en este.

- ✓Fortalecer los mecanismos de control y validación periódica de la información y las evidencias del MSPI, en coherencia con los lineamientos emitidos por el MINTIC.

- ✓Realizar un análisis integral de la gestión de riesgos de seguridad de la información que permita actualizar el registro de incidentes y la matriz de riesgos vigente, y consolidar en Isolucion los planes de mejoramiento derivados de las auditorías y hallazgos del modelo.

- ✓Depurar en Isolucion los documentos asociados a la gestión tecnológica de la entidad, ajustándolos al Mapa de Procesos vigente, y establecer un control que asegure su actualización permanente.

Para constancia se firma en Bogotá D.C., a los 3 días del mes de septiembre del año 2026.

APROBACIÓN DEL INFORME DE AUDITORÍA		
Nombre Completo	**Responsabilidad** (cargo)	**Firma**
Wilma Rocío Bejarano Gaitán	Jefe Oficina de Control Interno	BEJARANO GAITAN WILMA ROCIO Firmado digitalmente por BEJARANO GAITAN WILMA ROCIO Fecha: 2026.09.03 16:35:21 -05'00'
Juan David Parga	Contratista	
Alcenides Martínez	Contratista	
Diego Urazán Franco	Contratista