TABLA DE CONTENIDO

INDICE DE TABLAS

INDICE DE ABREVIATURAS

SIGLA	SIGNIFICADO
ANT	Agencia Nacional de Tierras
CI	Control Interno
CICCI	Comité Institucional de Coordinación de Control Interno
DRP	(Disaster Recovery Plan) Plan de Recuperación ante Desastres.
NC	No Conformidad
C	Conformidad
GINFO	Gestión de la Información
INTI	Inteligencia de la Información
ISO	International Organization for Standardization
MECI	Manual Estándar de Control Interno.
MinTIC	Ministerio de Tecnologías de la Información y Comunicaciones
MIPG	Modelo Integrado de Planeación y Gestión.
MSPI	Modelo de Seguridad y Privacidad de la Información
NIST	National Institute of Standards and Technology
NOC	(Network Operations Center) Centro de Operaciones de Red
PHVA:	Planear – Hacer – Verificar – Actuar
SGSI	Sistema de Gestión de Seguridad de la Información
SOC	SOC (Security Operations Center) Centro de Operaciones de Seguridad.
SSIT	Subdirección de Sistemas de Información de Tierras.
TIC:	Tecnologías de la Información y las Comunicaciones
UGT	Unidad de Gestión Territorial

1. INFORMACIÓN GENERAL

Tipo de informe	**Preliminar ( ) Final (X)**	**Fecha de emisión**	**04**	**09**	**2025**
Dependencia y/o proceso auditado	Subdirección Sistemas de Información de Tierras				
Título de la actividad	Auditoria Modelo de Seguridad y Privacidad de la Información				
Objetivo	Evaluar el Modelo de Seguridad y Privacidad de la Información (MSPI) implementado en la Agencia, mediante el análisis de sus políticas, procedimientos, controles y mecanismos de protección, con base en estándares internacionales, normativas legales aplicables y buenas prácticas en gestión de seguridad y privacidad, para determinar su efectividad, identificar riesgos, brechas o incumplimientos, y proponer oportunidades de mejora que fortalezcan la protección de los activos de información y aseguren el cumplimiento de los requisitos legales e institucionales				
Alcance	La auditoría comprende la verificación de los siguientes aspectos: ➢ Revisión de los componentes estructurales del MSPI, con relación al diagnóstico de seguridad y privacidad de la información, la Política del MSPI, la asignación de roles y responsabilidades, los procedimientos de seguridad de la información, la gestión de activos de información y la gestión de riesgos de seguridad y privacidad. ➢ Verificación de los controles operacionales y medición del desempeño del MSPI, respecto a la implementación efectiva de los controles definidos para mitigar o reducir los riesgos identificados; la existencia de procedimientos operativos documentados que respalden su aplicación; evidencias de cumplimiento (registros, revisiones, resultados de monitoreo); alineación de los controles con los objetivos institucionales de seguridad de la información; y el uso de indicadores clave de desempeño que permitan monitorear la eficacia del sistema. ➢ Evaluar el seguimiento y mejora continua del MSPI, en torno a la existencia y efectividad de los mecanismos establecidos para el seguimiento del desempeño del Sistema de Gestión de Seguridad de la Información (SGSI), incluyendo acciones correctivas ante hallazgos y la implementación de un enfoque de mejora continua, en concordancia con los principios de gestión por procesos, los lineamientos del MSPI.				

	Análisis en las áreas y procesos críticos que manejan información sensible o confidencial dentro de la Agencia, considerando el estado actual de implementación del MSPI.
Limitaciones	La actividad de aseguramiento no presentó limitaciones para el desarrollo de las pruebas de auditoría establecidas.

2. METODOLOGIA

2.1. Contexto Modelo de Seguridad y Privacidad de la Información - MSPI

El Modelo de Seguridad y Privacidad de la Información (MSPI), adoptado en el marco de la Política de Gobierno Digital, es una herramienta que orienta a las entidades públicas en la gestión integral de la seguridad de la información y la protección de datos personales. Su propósito es asegurar que la información institucional, en todas las etapas de su ciclo de vida, se administre con criterios de confidencialidad, integridad, disponibilidad y trazabilidad, en concordancia con estándares nacionales e internacionales.

En el caso de la Agencia Nacional de Tierras, el autodiagnóstico institucional de 2024 mostró que la entidad se encuentra aún en una fase temprana de adopción del modelo, sin alcanzar el nivel de madurez inicial. Esto significa que ya existen avances importantes, como la formulación de políticas y la definición de roles, pero todavía quedan aspectos por fortalecer en la implementación práctica, en el seguimiento al desempeño y en la consolidación del mejoramiento continuo.

2.2. Metodología de la actividad de aseguramiento

La auditoría al Modelo de Seguridad y Privacidad de la Información se desarrolló en cumplimiento del Plan Anual de Auditorías 2025, aprobado por el Comité Institucional de Coordinación de Control Interno (CICCI) en sesión del 17 de marzo de 2025. El proceso inició formalmente con la reunión de apertura, realizada de manera presencial el 26 de mayo de 2025, con la participación de la subdirectora de la Subdirección de Sistemas de Información de Tierras y del personal responsable de la gestión del MSPI. En esta sesión se presentó y acordó el programa de auditoría definido por la Oficina de Control Interno.

El programa de auditoría contempló dos alcances sucesivos:

- El primero, definido el 23 de julio de 2025, en atención a la capacidad operativa de la Oficina de Control Interno.
- El segundo, establecido el 11 de agosto de 2025, con ocasión de la programación de la visita a la UGT Pasto.

Con el propósito de garantizar la confidencialidad, objetividad e independencia, el equipo auditor suscribió el acuerdo de confidencialidad y declaración de no conflictos (formato SEYM-F-009), mientras que los directivos responsables firmaron la carta de representación (formato SEYM-F-010).

La actividad de aseguramiento comprendió el cotejo de los criterios de auditoría establecidos en el programa, aplicando pruebas de cumplimiento y de procedimiento que permitieron un análisis detallado de la implementación del MSPI. Dichas actividades se llevaron a cabo siguiendo metodologías y técnicas basadas en las mejores prácticas internacionales de auditoría (IIA e ISO 19011), manteniendo comunicación permanente con los responsables de las áreas auditadas para resolver inquietudes y validar evidencias, a través de entrevistas presenciales, virtuales y telefónicas.

Los resultados presentados en este informe se sustentan en la información recopilada y verificada durante el trabajo de campo, documentada de manera completa y transparente, de modo que los interesados puedan comprender con claridad las conclusiones alcanzadas. Se incluyen tanto las conformidades como las no conformidades, así como las oportunidades de mejora identificadas, y se formulan recomendaciones específicas orientadas a fortalecer los controles internos y optimizar la gestión de recursos.

El proceso se adelantó bajo los principios de ética, objetividad y profesionalismo, asegurando que la auditoría cumpliera con los estándares de calidad, independencia y confiabilidad requeridos para este tipo de evaluaciones.

En concordancia con la metodología expuesta, y con el fin de garantizar la trazabilidad de las evidencias frente a los criterios definidos en el programa de auditoría, el equipo auditor aplicó un conjunto de pruebas de auditoría estructuradas. Estas pruebas permitieron contrastar la información obtenida mediante entrevistas, revisión documental, análisis de registros y observación directa, con los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI). A continuación, se presentan las pruebas aplicadas, junto con las conformidades y no conformidades identificadas en cada caso, lo que ofrece una visión integral del grado de cumplimiento alcanzado por la entidad en la implementación del modelo.

2.3. Prueba a la fase de Diagnóstico y Planificación

La prueba tuvo como propósito verificar la existencia, aplicación y trazabilidad de los elementos establecidos en la fase de Diagnóstico y Planificación del MSPI, asegurando que la entidad hubiera definido su contexto organizacional, identificado los activos de información e infraestructura crítica, valorado los riesgos de seguridad de la información y formulado los planes de tratamiento

correspondientes. Asimismo, se buscó comprobar la alineación de estos elementos con los lineamientos del Documento Maestro del MSPI y su coherencia con los objetivos institucionales. Los temas analizados fueron los siguientes:

- **Diagnóstico.** Se revisó la aplicación del instrumento de autodiagnóstico del MSPI como punto de partida para establecer la línea base, medir el nivel de madurez institucional y formular acciones de mejora.
- **Contexto.** Se verificó la comprensión de la organización y su entorno, la identificación de partes interesadas relevantes y la definición formal del alcance del modelo.
- **Liderazgo.** Se evaluó la inclusión de funciones de seguridad y privacidad en el Comité Institucional de Gestión y Desempeño, la formulación de la política del MSPI y la definición de roles y responsabilidades con delegación formal del responsable de seguridad de la información.
- **Planificación.** Se analizó la identificación y clasificación de activos de información e infraestructura crítica, la valoración de riesgos de seguridad de la información y la formulación del plan de tratamiento de riesgos.
- **Soporte.** Se verificó la disposición de recursos financieros, humanos y tecnológicos para la implementación del MSPI, así como las acciones de capacitación, sensibilización, comunicación y concienciación en materia de seguridad de la información.

A partir de la revisión realizada en esta fase, se identificaron tanto conformidades que reflejan buenas prácticas en la implementación del modelo, como no conformidades que evidencian aspectos a mejorar. Estos resultados se desarrollan en los siguientes hallazgos:

Conformidades:

- **Conformidad Nro. 1.** Aplicación y trazabilidad del diagnóstico del MSPI como insumo para la planificación y el seguimiento del modelo.
- **Conformidad Nro. 2.** Inclusión de funciones relacionadas con seguridad y privacidad de la información en el Comité Institucional de Gestión y Desempeño.
- **Conformidad Nro. 3.** Cumplimiento en Procedimientos de Seguridad de la Información.
- **Conformidad Nro. 4.** Cumplimiento en la articulación de roles institucionales y en la delegación formal del responsable de seguridad y privacidad de la información.
- **Conformidad Nro. 5.** Cumplimiento en la Identificación de activos de información e infraestructura crítica.
- **Conformidad Nro. 6.** Cumplimiento en la valoración de riesgos de seguridad de la información.
- **Conformidad Nro. 7.** Disponibilidad y suficiencia de recursos para el MSPI.

No Conformidades:

- **No Conformidad Nro. 1.** Debilidades en el avance de la implementación del MSPI.
- **No Conformidad Nro. 2.** Debilidades en la definición específica del contexto de la entidad conforme al MSPI.
- **No Conformidad Nro. 3.** Debilidades en la determinación de partes interesadas relevantes para la Seguridad de la Información.
- **No Conformidad Nro. 4.** Debilidades en la definición formal y aprobación del alcance del MSPI.
- **No Conformidad Nro. 5.** Debilidades en el liderazgo y compromiso del Comité Institucional de Gestión y Desempeño frente al MSPI.
- **No Conformidad Nro. 6.** Debilidades en la documentación, aprobación, comunicación y alineación de la Política del MSPI con los objetivos institucionales.
- **No Conformidad Nro. 7.** Debilidades en el esquema institucional de roles y responsabilidades para la implementación del MSPI.
- **No Conformidad Nro. 8.** Debilidades en el plan de comunicación, capacitación, sensibilización y concientización.

2.4. Prueba a la fase de Operación

La prueba tuvo como propósito verificar la implementación de los controles definidos en el plan de tratamiento de riesgos de seguridad de la información, asegurando que las acciones priorizadas fueran formalizadas, documentadas y puestas en marcha con el aval del Comité Institucional de Gestión y Desempeño. Se buscó establecer si la Agencia Nacional de Tierras contaba con evidencia suficiente de ejecución práctica y seguimiento de los planes aprobados. De acuerdo con lo previsto en el Documento Maestro del MSPI (numeral 8.1 – Planificación e implementación) y la evidencia revisada en el informe de auditoría, se analizaron los siguientes aspectos:

- **Plan de tratamiento de riesgos**. Verificación de su aprobación, actualización y coherencia con los inventarios de activos y la valoración de riesgos realizada.
- **Planificación e implementación de controles**. Análisis de la metodología definida para ejecutar los controles de seguridad y privacidad, así como su alineación con estándares internacionales como ISO/IEC 27001.
- **Evidencias de implementación**. Revisión de documentos, registros y mecanismos que demuestran la puesta en marcha de los controles sobre activos críticos de información.
- **Aprobación institucional**. Confirmación del respaldo formal del Comité Institucional de Gestión y Desempeño a los planes de tratamiento y controles adoptados.

En esta fase se evidenciaron conformidades que demuestran avances en la ejecución del modelo, así como no conformidades que ponen de manifiesto debilidades en su implementación práctica. Estos resultados se desarrollan en los siguientes hallazgos:

Conformidades:

- **Conformidad Nro. 8.** Cumplimiento en la formulación del Plan de tratamiento de los riesgos de seguridad de la información.

No conformidades:

- **No Conformidad Nro. 9.** Debilidades en la planificación e implementación de controles.

2.5. Prueba a la fase de Evaluación de Desempeño

La prueba tuvo como propósito verificar si la entidad evalúa de manera sistemática la efectividad del MSPI, mediante el uso de indicadores de seguimiento, la ejecución de auditorías internas y la revisión periódica por parte de la alta dirección. Se buscó comprobar que estas actividades estén formalmente planificadas, documentadas y alineadas con los requerimientos del modelo y del MIPG. De acuerdo con el Documento Maestro del MSPI y el informe de auditoría, se revisaron los siguientes aspectos:

- **Seguimiento, medición, análisis y evaluación.** Existencia de indicadores para medir la eficacia de los controles y resultados obtenidos.
- **Auditoría interna.** Ejecución de auditorías internas al MSPI, aprobación del plan anual de auditoría y cumplimiento del cronograma.
- **Revisión por la dirección.** Realización de revisiones periódicas por la alta dirección y registro de compromisos derivados de dichas sesiones.

Durante esta fase se identificaron Conformidades que muestran avances en el cumplimiento de los requisitos del modelo, junto con No Conformidades que reflejan vacíos en su seguimiento y control. Estos resultados se desarrollan en los siguientes hallazgos:

Conformidades:

- **Conformidad Nro. 9.** Cumplimiento del requisito de auditoría interna del MSPI con planificación y aprobación formal.

No Conformidades:

- **No Conformidad Nro. 10.** Debilidades en el seguimiento, medición, análisis y evaluación del MSPI.

- **No Conformidad Nro. 11.** Debilidades en la revisión por la dirección del MSPI.

2.6. Prueba a la fase de Mejoramiento Continuo

La prueba tuvo como propósito verificar si la entidad cuenta con un plan de mejoramiento continuo en materia de seguridad y privacidad de la información. El objetivo fue constatar que la Agencia Nacional de Tierras diseñará e implementará acciones correctivas y preventivas orientadas a mitigar debilidades, optimizar controles y elevar el nivel de madurez del MSPI. De acuerdo con el Documento Maestro del MSPI y la evidencia revisada, se evaluaron los siguientes aspectos:

- **Consolidación de resultados de la evaluación de desempeño.** Inclusión de hallazgos, indicadores y revisiones como insumo para la mejora.
- **Plan Anual de Mejora del MSPI.** Existencia, aprobación y ejecución del plan, con actividades concretas, responsables y plazos definidos.
- **Acciones correctivas y preventivas.** Definición de medidas específicas para subsanar no conformidades y prevenir su reincidencia.
- **Optimización de procesos y controles.** Implementación de mejoras que eleven la madurez del modelo y fortalezcan la cultura de seguridad de la información.

En la fase de mejoramiento continuo se identificó una No Conformidad relacionada con la ausencia del plan anual de mejora, lo que limita la capacidad de la entidad para garantizar la implementación sistemática de acciones correctivas y preventivas. Ver **No Conformidad Nro. 12.** Debilidades en el Plan Anual de Mejora del MSPI.

- **Visita UGT Pasto**

En el marco de la auditoría al MSPI se efectuó una visita de verificación a la Unidad de Gestión Territorial (UGT) Pasto, con el fin de evaluar en sitio el nivel de conocimiento, apropiación y cumplimiento de las responsabilidades asignadas a funcionarios y contratistas en materia de seguridad de la información.

La comisión permitió adelantar entrevistas y encuestas para constatar el entendimiento sobre las disposiciones del modelo, la asistencia a actividades de capacitación, la aplicación de controles en el manejo de activos de información y el conocimiento del procedimiento de reporte de incidentes. Así mismo, se revisaron las condiciones locales de operación, lo cual aportó evidencia directa sobre la forma en que se gestionan los lineamientos del MSPI en una dependencia territorial.

Selección de la Muestra

Para seleccionar la muestra de los contratistas (79) de la UGT Pasto la OCI utilizó el método coordinado negativo, después de haber determinado el tamaño de la muestra necesario. El método coordinado negativo, también conocido como muestreo aleatorio sistemático negativo, es una técnica que selecciona muestras utilizando un intervalo de selección fijo, pero comenzando desde un punto de partida aleatorio. Este método es especialmente útil cuando se desea una dispersión uniforme de la muestra a través del conjunto de datos, lo que es relevante donde cada registro tiene un equivalente digital o físico en un orden específico.

Generación de Números Aleatorios: Para cada elemento de la población, se genera un número aleatorio desde una distribución uniforme entre 0 y 1. Esto significa que cada elemento tiene la misma probabilidad de ser elegido, asegurando la aleatoriedad y la equidad en la selección.

- **Asignación de números aleatorios a cada elemento.** Cada elemento de la población se asocia con el número aleatorio generado en el paso anterior.
- **Ordenación de elementos.** Los elementos de la población son ordenados de forma ascendente o descendente basados en los números aleatorios asignados. Este ordenamiento no afecta las probabilidades, pero facilita la selección de una muestra.
- **Selección de la muestra.** Dependiendo del tamaño de la muestra deseado, se seleccionan los primeros n elementos de la lista ordenada como la muestra. Esto garantiza que cada elemento tenga la misma probabilidad de ser incluido en la muestra final. Este procedimiento asegura que todos los elementos de la población tengan la misma oportunidad de ser seleccionados, haciendo que la muestra sea un buen reflejo de la población total. Esto es crucial para la validez de los análisis estadísticos subsecuentes basados en la muestra seleccionada.

De esta manera, la visita complementó el trabajo realizado en la sede central, ofreciendo una visión integral de la implementación del modelo en la entidad y permitiendo identificar tanto fortalezas como aspectos susceptibles de mejora en la apropiación institucional del MSPI.

Los resultados alcanzados hacen parte de la **No Conformidad Nro. 13** Debilidades en la implementación de procedimientos de seguridad de la información UGT Pasto.

3. HALLAZGOS

A continuación, se presentan los resultados con cumplimiento e incumplimiento de los criterios establecidos para la auditoría:

3.1. REQUISITOS CON CUMPLIMIENTO – CONFORMIDADES

3.1.1. CONFORMIDAD Nro. 1. Aplicación y trazabilidad del diagnóstico del MSPI como insumo para la planificación y el seguimiento del modelo.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI) – MinTIC.**

Numeral 6. Diagnóstico.

- **Instructivo de diligenciamiento del diagnóstico MSPI – MinTIC.**

Numeral 5. Requisitos técnicos para el uso del instrumento de evaluación.

CONDICIÓN OBSERVADA:

La Agencia Nacional de Tierras aplicó el instrumento de autodiagnóstico definido por el MinTIC durante la vigencia 2023 como punto de partida para establecer su línea base, y actualizó el mismo instrumento con corte al año 2024, en cumplimiento del ciclo establecido en el Modelo de Seguridad y Privacidad de la Información (MSPI). En ambas vigencias, los instrumentos de evaluación del MSPI presentan sus hojas estructuradas conforme a los lineamientos establecidos por el MinTIC, incluyendo el análisis del avance del modelo, los niveles de madurez y los porcentajes de cumplimiento de los controles. Asimismo, frente a las brechas identificadas, se evidenció la formulación de acciones de mejora.

ANALISIS:

La Agencia Nacional de Tierras (ANT), a través de la Subdirección de Sistemas de Información de Tierras (SSIT), aplicó el instrumento de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) en dos momentos clave del ciclo de gestión:

- El **autodiagnóstico de línea base**, con fecha de aplicación **3**1 de diciembre de 2023, documentado en el archivo *"Autodiagnóstico_Instrumento_Evaluación_MSPI 2023"*, y
- El **autodiagnóstico correspondiente a la fase de evaluación de desempeño**, con fecha de aplicación 14 de agosto de 2024, contenido en el archivo *"Instrumento_Evaluacion_MSPI_ANT_2024"*.

Ambos archivos fueron remitidos inicialmente mediante correo electrónico del 29 de mayo de 2025 y complementados, a solicitud del equipo auditor, el 20 de junio de 2025, junto con el archivo *"Plan Cierre de Brechas MSPI - Seguimiento 2025"*.

Del análisis de las evidencias se concluye que, en ambas vigencias, se empleó el instrumento oficial de autodiagnóstico establecido por el MinTIC, el cual contempla los componentes estructurales requeridos: evaluación de controles administrativos y técnicos, aplicación del ciclo PHVA, medición del nivel de madurez y evaluación de controles de ciberseguridad.

En el diagnóstico de 2023 se reporta un avance del 29% en el modelo de operación, con niveles de madurez clasificados como "Inicial" (suficiente) y "Repetible" (intermedio), mientras que los niveles "Definido", "Administrado" y "Optimizado" fueron calificados como críticos. El cumplimiento de controles fue del 43%.

En la versión 2024, se reporta un avance del 31%, manteniéndose los mismos niveles de madurez. El cumplimiento de controles fue del 41%. Esta versión fue actualizada el 20 de junio de 2025, incluyendo vínculos a evidencias de soporte para cada uno de los 42 controles evaluados.

Asimismo, se recibió el documento *"Informe Nivel de Madurez MSPI ANT 2023"*, correspondiente al diagnóstico de 2023, y el *"Informe Autodiagnóstico_MSPI_ANT_2024"*, que resume los resultados de la vigencia 2024. Ambos informes reflejan los resultados del análisis GAP, identificando brechas por dominio y acciones de mejora, en concordancia con el propósito establecido para la fase de diagnóstico.

Los instrumentos cumplen estructuralmente con los requerimientos establecidos en el numeral 5 del Instructivo Técnico del MinTIC, salvo por omisiones formales en las hojas "Portada" y "Levantamiento de información" (como el nombre y contacto del responsable y el rango de fechas de evaluación).
Adicionalmente, la SSIT entregó el archivo "Plan Cierre de Brechas MSPI - Seguimiento 2025", que contiene acciones formuladas frente a los resultados observados en el diagnóstico. También se evidenció la socialización institucional del diagnóstico 2024 mediante el Acta No. 4 del Comité Institucional de Gestión y Desempeño, con fecha 19 de diciembre de 2024.

No obstante, del comparativo entre los diagnósticos 2023 y 2024, se identificó que varios controles presentan una disminución en su calificación de cumplimiento. Esta situación, aunque no impide calificar la práctica como conforme, sugiere la necesidad de revisar la consistencia metodológica aplicada en las evaluaciones, así como el seguimiento efectivo de las acciones de mejora.

Aunque se identificaron oportunidades de mejora, como el diligenciamiento incompleto de campos relacionados con el responsable del diagnóstico, las fechas precisas de inicio y cierre, y una mayor articulación entre los documentos de análisis y sus respectivas fuentes de evidencia, estos aspectos no comprometen el cumplimiento del criterio de auditoría.

En este sentido, se concluye que la entidad ha cumplido con la ejecución de la fase de diagnóstico del MSPI, conforme a los lineamientos del MinTIC y al numeral 6 del Documento Maestro del Modelo. No obstante, se formulan recomendaciones y se identifican posibles riesgos asociados a los aspectos por fortalecer.

3.1.2. CONFORMIDAD Nro. 2. Inclusión de funciones relacionadas con seguridad y privacidad de la información en el Comité Institucional de Gestión y Desempeño.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI) – MinTIC.**

Numeral 7.2.1. Liderazgo y Compromiso

- Acto administrativo que soporta la conformación del comité de gestión y desempeño o quien haga sus veces, señalando las funciones de seguridad y privacidad de la información.

CONDICIÓN OBSERVADA:

La Agencia Nacional de Tierras formalizó mediante la Resolución No. 183 del 9 de febrero de 2018 la conformación y funciones del Comité Institucional de Gestión y Desempeño. Dentro de las funciones asignadas se encuentra la de formular políticas y directrices en materia de seguridad digital y de la información, lo que proporciona un marco normativo que puede abarcar aspectos relacionados con la seguridad y privacidad de la información en el contexto del MSPI.

ANÁLISIS:

La Resolución No. 183 de 2018, entregada por la Oficina de Planeación como soporte normativo del MSPI, establece competencias del Comité en temas de gobernanza de la información. Si bien no menciona explícitamente el MSPI, ni responsabilidades específicas como la adopción, implementación o mejora continua del modelo, sí incluye lineamientos generales sobre seguridad digital y de la información que resultan coherentes con los principios del MSPI.

Es importante precisar que esta resolución fue expedida antes del establecimiento formal del MSPI por el MinTIC, lo que explica la ausencia de referencias al modelo y a sus componentes técnicos (diagnóstico, plan de cierre de brechas, ciclo PHVA, etc.). En consecuencia, puede considerarse que el acto administrativo constituye una base normativa suficiente en términos generales, pero limitada en cuanto a la especificidad que hoy exige el MSPI.

Se concluye que, la existencia de la Resolución No. 183 de 2018 permite dar cumplimiento general al criterio de contar con un acto administrativo que soporta la conformación del Comité y sus funciones en seguridad de la información. Sin embargo, las limitaciones señaladas evidencian la necesidad de una actualización normativa para fortalecer la alineación con el MSPI y garantizar que el Comité ejerza un rol explícito y trazable en la gestión de seguridad y privacidad de la información.

3.1.3. CONFORMIDAD Nro. 3. Cumplimiento en Procedimientos de Seguridad de la Información.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI) – MinTIC**.

Numeral 8.1. Planificación e Implementación.

- **INTI-Política-001** Política General de Seguridad y Privacidad de la Información, versión 5 del 29/10/2024.
- **INTI-M-001** Manual Sistema de Gestión de Seguridad de la Información, versión 1 del 30/12/2024.
- **INTI-Política-008** Lineamientos de Seguridad de la Información, versión 4 del 20/12/2024.
- **INTI-Política-011** Política de Protección de Datos Personales, versión 3 del 29/10/2024.
- **GINFO-P-011** Procedimiento Gestión de Incidentes de Seguridad de la Información, versión 1 del 3/11/2020.

CONDICION OBSERVADA:

La Agencia Nacional de Tierras cuenta con un conjunto elementos para la seguridad de la información, compuesto por política, gestión documental, análisis de riesgos, controles internos, procedimientos y

procesos de mejora continua. Esto demuestra un enfoque integral para proteger la información, alineado con estándares nacionales y mejores prácticas.

ANALISIS:

- **Manual del Sistema de Gestión de Seguridad de la Información y Lineamientos de Seguridad de la Información.**

De acuerdo con la revisión realizada, se observó que el Manual como los Lineamientos están concebidos como instrumentos de soporte a la Política General de Seguridad y Privacidad de la Información, alineándose con la estrategia de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información – MSPI y el marco legal Ley 1581 de 2012 (Ley de Protección de Datos Personales), Ley 1712 de 2014 (Ley de Transparencia y del Derecho de Acceso a la Información Pública).

La Política General de Seguridad y Privacidad de la Información (INTI-Política-001) establece principios como la protección de la confidencialidad, integridad y disponibilidad de la información, el fortalecimiento de la cultura de seguridad y la gestión de riesgos. Estos son abordados de manera operativa en:

- El INTI-M-001 Manual Sistema de Gestión de Seguridad de la Información, mediante la definición del ciclo PHVA aplicado a la seguridad, la contextualización interna y externa, el análisis de riesgos y la mejora continua.
- Los Lineamientos de Seguridad de la Información, mediante instrucciones específicas sobre responsabilidades, uso aceptable, clasificación y etiquetado, control de dispositivos móviles, protección legal, gestión de talento humano y respuesta a incidentes.

La política remite expresamente al documento de INTI-Política-008 Lineamientos de Seguridad de la Información v4 como su desarrollo técnico y organizacional. A su vez, los lineamientos refieren al Manual del SGSI como base estructural del sistema, lo cual evidencia una integración documental coherente y jerarquizada.

Asimismo, se observó asignación de responsabilidades y gobernabilidad, los tres documentos contemplan un sistema robusto de gobernabilidad en cuanto a:

- **Alta dirección:** compromiso con el SGSI y provisión de recursos.
- **Oficial de Seguridad:** rol técnico de articulación, vigilancia, reporte y coordinación. Para lo cual se observó que, mediante resolución 202361002101356 del 23/09/2023, el Director General de

la Agencia Nacional de Tierras- ANT asignó como responsable al jefe de la Subdirección de Sistemas de Información de Tierras (SSIT).

- **Funcionarios, contratistas y terceros:** sujetos obligados a cumplir con la política y controles, incluyendo deberes de confidencialidad, uso adecuado y reporte de incidentes.

Así mismo, la política de Seguridad de la Información exige definir controles técnicos, administrativos y legales.

Conforme a la verificación por parte de la Oficina de Control Interno se refleja su operatividad teniendo en cuenta:

- El Manual del SGSI, describe el tratamiento de riesgos, amenazas, vulnerabilidades y controles mediante un enfoque de mejora continua.
- Los lineamientos, detallan prácticas como la clasificación de la información, inventario de activos, segregación de funciones, tratamiento disciplinario y medidas preventivas.

La Oficina de Control Interno concluye que tanto los Lineamientos de Seguridad de la Información como el Manual del SGSI de la ANT soportan adecuadamente la implementación de la Política General de Seguridad y Privacidad de la Información. Existe una correspondencia lógica y funcional entre los tres documentos, que permite establecer un marco sólido y coherente para la gestión de la seguridad de la información, de conformidad con los requerimientos del MSPI.

➢ **Procedimiento GINFO-P-011 Gestión de Incidentes de Seguridad de la Información.**

De acuerdo con GINFO-P-011 versión 1 del 3/11/2020 Procedimiento Gestión de Incidentes de Seguridad de la Información, GINFO-G-006-Guía de Gestión de Incidentes de Seguridad de la Información versión 1 del 03/11/2020 y GINFO-F-028-Registro de Incidentes de Seguridad de la Información versión 1 del 03/1/2020, el procedimiento define el proceso de reporte, análisis, tratamiento y cierre de incidentes, lo que responde a necesidades típicas de interesados como usuarios internos, Tecnologías de Información, entes de control y ciudadanía. De igual forma se observó responsables definidos, canales de reporte y tiempos de respuesta contemplados, lo que contribuye a la trazabilidad y respuesta ante eventos que puedan afectar la información institucional.

Con base en el análisis, se puede indicar que el Procedimiento GINFO-P-011 de Gestión de Incidentes de Seguridad de la Información de la ANT soporta adecuadamente la implementación de los Lineamientos de Seguridad de la Información (INTI-Política-008) en cuanto a:

- **Coherencia con la INTI-Política-008 Lineamientos de Seguridad de la Información y el SGSI.**

El procedimiento está alineado con los principios de confidencialidad, integridad y disponibilidad definidos en los Lineamientos de Seguridad de la Información, así como con los lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI) y el MSPI donde el objetivo del procedimiento es coherente con el propósito del SGSI definido en el manual y los lineamientos.

- **Responsabilidad organizacional.**

El INTI-Política-008 Lineamientos de Seguridad de la Información establece roles y responsabilidades como las del Oficial de Seguridad de la Información, funcionarios y contratistas. El procedimiento opera de acuerdo con las responsabilidades y actividades asignadas a los actores clave, como: Oficial de Seguridad o quien haga sus veces, el Equipo de Infraestructura y Soporte Tecnológico y responsables del activo afectado.

- **Vinculación con controles y mejora continua.**

Los Lineamientos de Seguridad de la Información exigen una gestión proactiva, basada en riesgos y controles. El procedimiento detalla tareas como:
Contención y erradicación, Notificación y cierre, Revisión post-incidente, Registro en formatos institucionales como GINFO-F-028 Registro de Incidentes de Seguridad de la Información v1 03/1/2020.

Sin embargo, el documento tiene fecha de noviembre de 2020, y no se evidencia su actualización frente a nuevas regulaciones o cambios institucionales, lo que podría implicar una desalineación con necesidades actuales.

- **Cumplimiento normativo.**

Ambos documentos se sustentan en la normatividad aplicable, incluyendo ISO/IEC 27001:2013, Decreto 1008 de 2018 y Decreto 2573 de 2014, Ley 1581 de 2012 (protección de datos) y Ley 23 de 1982 (derechos de autor).

- **GINFO-G-006-Guía de Gestión de Incidentes de Seguridad de la Información, versión 1 del 03/11/2020.**

De conformidad con la Guía de Gestión de Incidentes de Seguridad de la Información detalla cómo actuar ante eventos que afecten confidencialidad, integridad o disponibilidad, lo cual es coherente con lo que esperan los interesados.

- **GINFO-F-028-Registro de Incidentes de Seguridad de la Información, versión 1 del 03/1/2020.**

El formato GINFO-F-028 permite registrar detalles esenciales del incidente (fecha, descripción, clasificación, acciones tomadas), lo que habilita la trazabilidad y seguimiento, aspectos clave para auditores, responsables y víctimas de incidentes.

- **Protección de datos personales**

A continuación, se presenta un análisis de la Política de Protección de Datos Personales de la Agencia Nacional de Tierras (ANT) versión 3, en relación con los requisitos del Modelo de Seguridad y Privacidad de la Información (MSPI):

La Agencia Nacional de Tierras cuenta con la Política de Protección de Datos Personales INTI-Política-011 v 3 de 29/10/2024.

En relación con los requisitos del Modelo de Seguridad y Privacidad de la Información (MSPI) particularmente en su componente de protección de datos personales y cumplimiento normativo, la política presenta cumplimiento en cuanto a:

- La política incorpora de forma explícita la aplicación de Responsabilidad Demostrada, el marco normativo en seguridad y privacidad de la información y hace referencia a la guía de la SIC. Se asignan funciones formales a la Subdirección de Sistemas de Información como Oficial de Datos Personales, mediante acto administrativo interno Resolución 202361002101356 del 04/09/2023, en cumplimiento del numeral 7.2.3 Roles y responsabilidades.
- La política desarrolla las definiciones esenciales (dato personal, tratamiento, transferencia, transmisión) y enlista el marco normativo aplicable (Constitución, Ley 1581, Decretos reglamentarios) e Inclusión del tratamiento de datos sensibles y de menores de edad.
- Se identifican claramente los datos de contacto de la ANT como responsable del tratamiento, incluyendo canales de atención física, electrónica y virtual.
- Conforme al ítem 7.3.3 Plan de tratamiento de riesgos de seguridad de la información se visualiza como activo de información “Datos Personales” asociando a este los riesgos 26 al 31. Se evidencia la implementación de un proceso formal y documentado de valoración de riesgos específicos para la protección de datos personales.

- Se especifican claramente las finalidades del tratamiento de datos personales, desde la recolección hasta la supresión, detallando las actividades misionales, contractuales y de gestión interna conforme al numeral 8.1 del MSPI.
- Conforme al ítem 10.1 Mejora continua no se evidencia explícitamente.
- La política se soporta en el SGSI, pero no describe un procedimiento detallado para incidentes sobre datos personales.

La Política de Protección de Datos Personales de la ANT versión 3 cumple en gran medida con los requerimientos del MSPI en cuanto a legalidad, gestión de derechos, tratamiento integral de la información y medidas de seguridad. No obstante, se recomienda reforzar la trazabilidad del cumplimiento y la articulación explícita con el MSPI para fortalecer la gobernanza de la seguridad de la información.

3.1.4. CONFORMIDAD Nro. 4. Cumplimiento en la articulación de roles institucionales y en la delegación formal del responsable de seguridad y privacidad de la información.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI). Numeral 7.2.3.** Roles y responsabilidades.

- Articular con las áreas o dependencias de la entidad, los roles y responsabilidades necesarios para la adopción del MSPI.
- Delegar a un responsable de la seguridad y privacidad de la información; si el cargo no existe, debe ser delegado por acto administrativo y depender de un área estratégica distinta a la Oficina de Tecnología (se recomienda el despacho del nominador).

CONDICIÓN OBSERVADA:

En la verificación realizada sobre el numeral 7.2.3 del Documento Maestro del MSPI, se determinó que la entidad cumple en cuanto a la articulación con las dependencias para la definición de roles y responsabilidades necesarios para la adopción del modelo, así como en la delegación formal, mediante acto administrativo, de un responsable de la seguridad y privacidad de la información ubicado en un área estratégica distinta a la Oficina de Tecnología, garantizando con ello la independencia funcional, la trazabilidad institucional y la adecuada gobernanza en la implementación del MSPI.

ANÁLISIS:

En el marco de la verificación del numeral 7.2.3 Roles y Responsabilidades del Documento Maestro del MSPI, se estructuró una lista de chequeo con el fin de determinar el grado de cumplimiento de los lineamientos, propósitos y salidas establecidos. La verificación se centró en contrastar la evidencia documental y normativa disponible con los requisitos definidos en el modelo, identificando los aspectos conformes y aquellos que presentan brechas.

Del total de ítems evaluados, se identificaron dos casos conformes: el primero relacionado con la articulación de roles y responsabilidades entre las áreas de la entidad, y el quinto vinculado con la delegación formal del responsable de la seguridad y privacidad de la información. Para estos ítems, a continuación, se presenta un análisis detallado que sustenta la condición observada de conformidad, mientras que los demás hallazgos asociados al mismo numeral se documentan en la sección de no conformidades.

- **Articulación de roles y responsabilidades con las áreas de la entidad.**

Se verificó que el Manual INTI-M-001 Sistema de Gestión de Seguridad de la Información V1 (30/12/2024**)** incluye disposiciones que definen claramente los roles, responsabilidades y autoridades asignadas a diferentes instancias de la entidad, tales como:

- **Alta Dirección**: garantizar recursos, aprobar planes de seguridad, definir prioridades y ejercer liderazgo.
- **Oficial de Seguridad de la Información**: coordinar la implementación del MSPI, gestionar riesgos, realizar autodiagnósticos y coordinar la atención de incidentes.
- **Líderes de proceso**: responsables de los activos de información bajo su control, asegurando su clasificación, inventario y custodia.
- **Custodios de la información**: ejecutar los controles técnicos y administrativos para proteger los activos.
- **Funcionarios y contratistas**: cumplir políticas y lineamientos, custodiar la información a su cargo y reportar incidentes.

El documento plasma los roles como parte del diseño organizacional del MSPI, otorgándole trazabilidad y estructura jerárquica. Además, brinda una articulación transversal entre áreas, asignando responsabilidades compartidas en clasificación de activos, análisis de riesgos, gestión de incidentes, auditorías y capacitaciones. Este enfoque confirma que la seguridad de la información no se limita a un área técnica, sino que compromete a todo el ecosistema institucional.

En cuanto a la Política INTI-008 Lineamientos de Seguridad de la Información V4 (20/12/2024), los roles y responsabilidades se desarrollan en un nivel más operativo y normativo. Allí se establece:

- Que todos los funcionarios, contratistas y terceros deben asumir responsabilidades explícitas y medibles en seguridad de la información.
- La segregación de funciones para prevenir conflictos de interés.
- Responsabilidades específicas del Oficial de Seguridad de la Información, incluyendo ser enlace con autoridades externas (COLCERT, CSIRT, MinTIC, SIC), coordinar incidentes, gestionar riesgos y asegurar el cumplimiento de controles.
- Responsabilidades de áreas de apoyo como Jurídica (gestión normativa) y Talento Humano (formación, compromisos de confidencialidad, procesos disciplinarios en caso de incumplimiento).
- Responsabilidad de la Dirección en garantizar recursos, promover la cultura de seguridad y dar seguimiento a resultados.

➢ **Delegación del responsable de seguridad y privacidad de la información.**

Se evidenció que la entidad cumple con el criterio de designación formal de un responsable de seguridad y privacidad de la información. La Resolución No. 202361002101356 (04/09/2023) delega esta función en la Subdirectora Técnica de la Subdirección de Sistemas de Información de Tierras, quien asume el rol de Oficial de Seguridad de la Información y Seguridad Digital y de Protección de Datos Personales.

Este nombramiento satisface el requisito establecido en el numeral 7.2.3 del Documento Maestro del MSPI, dado que la designación se realizó mediante acto administrativo y el cargo delegado depende de un área estratégica distinta a la Oficina de Tecnología, garantizando independencia en la gestión del modelo. El organigrama institucional de 2025 confirma esta ubicación en la estructura organizacional.

No obstante, se observó que el alcance de la resolución se limita al rol individual de la Oficial de Seguridad y no abarca formalmente la designación de un equipo humano coordinador para apoyar la implementación del MSPI.

3.1.5. CONFORMIDAD Nro. 5. Cumplimiento en la Identificación de activos de información e infraestructura critica.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI). Numeral 7.3.1**. Identificación de activos de información e infraestructura critica.

- **INTI-Política-009** Lineamientos para la Gestión y Clasificación de Activos de Información, versión 3 del 10/02/2020.

CONDICIÓN OBSERVADA:

La entidad cuenta con el documento formal INTI-Política-009 – Lineamientos para la Gestión y Clasificación de Activos de Información, versión 3 del 10/02/2020, el cual establece directrices para la administración y categorización de los activos de información institucionales.

ANÁLISIS:

El documento INTI-Política-009-Lineamientos para la Gestión y Clasificación de Activos de Información V3 del 10/02/2020 establece criterios para:

- Inventario de activos.
- Calificación o clasificación de la información.
- Asignación de responsables y custodios.
- Protección de infraestructura crítica.

El documento se alinea con las guías de MinTIC, cumpliendo con lo requerido por el MSPI.

En cuanto a la implementación de un inventario de activos de información, **l**a ANT ha implementado un formato institucional INTI-F-020 Registro Activos de Información V2 del 29/08/2024 donde se registra:

- Nombre, tipo y descripción del activo.
- Ubicación.
- Nivel de calificación (confidencial, reservada, pública).
- Responsable y custodio del activo.

Este inventario permite la trazabilidad y evaluación periódica de los activos de información, y es revisado con una periodicidad definida semestral o anual, según los lineamientos.

Así mismo, la ANT tiene en cuenta la inclusión de activos de infraestructura crítica y dentro de los tipos de activos incluidos en el inventario institucional se tiene:

- Hardware (servidores, dispositivos críticos).
- Software.

- Sistemas de información y servicios esenciales (como la red de comunicaciones y bases de datos de ordenamiento territorial.

Esto garantiza que la infraestructura crítica también sea considerada como parte del proceso de identificación y valoración.

- **Articulación con el SGSI.**

El Manual del SGSI-INTI-M-001, establece que el alcance del sistema incluye desde la identificación y valoración de activos hasta la evaluación y mejora continua de su protección. Además, señala que la ANT adopta mecanismos para garantizar la confidencialidad, integridad y disponibilidad de los activos a lo largo de los procesos.

Se observó dentro de este el ítem 5.8 Inventario de Activos de Información y otros asociados a la misma donde refiere que:

(...)" e) El inventario de activos de información de la ANT debe ser exacto, actualizado, consistente y alineado con otros inventarios institucionales como: tablas de retención documental, clasificación de la información institucional, instrumentos de gestión pública de información, inventarios de infraestructura tecnológica e inventarios de activos fijos institucionales que sean formalizados mediante el comité institucional." (...)

Dentro del Portal de la ANT se encuentra INTI-F-020 Registro Activos de Información con fecha de publicación *10 de septiembre de 2024* ubicado en: https://www.ant.gov.co/transparencia-y-acceso-a-la-informacion-publica/datos-abiertos/instrumentos-de-gestion-de-la-informacion/registro-activos-de-informacion,

La Agencia Nacional de Tierras cumple con el Numeral 7.3.1 del MSPI en cuanto a la identificación de activos de información e infraestructura crítica. Se evidencia un proceso estructurado, documentado y en operación, que se encuentra articulado al SGSI institucional y alineado con los estándares del modelo de seguridad y normatividad vigente.

3.1.6. CONFORMIDAD Nro. 6. Cumplimiento en la valoración de los riesgos de seguridad de la información.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI).**

Numeral 7.3.2. Valoración de los riesgos de seguridad de la información

- **DEST-I-004** Instructivo para la Identificación y Valoración de Riesgos de Seguridad de la Información y valoración de controles existentes, versión de 19/09/2024.

- **Mapa de Riesgos de la Seguridad de la Información**, versión 2 – 2025 del 3/02/2025.

CONDICIÓN OBSERVADA:

En cumplimiento del numeral 7.3.2 del Modelo de Seguridad y Privacidad de la Información (MSPI), correspondiente a la valoración de los riesgos de seguridad de la información, se evidenció que la Agencia Nacional de Tierras (ANT) implementa de forma adecuada y conforme un proceso estructurado y formalmente documentado para la identificación, análisis y valoración de los riesgos asociados a los activos de información.

ANALISIS:

Conforme con la revisión realizada a los documentos aportados y disponibles en el SIG y el portal Web, la Oficina de Control Interno observó:

- **Política de Administración del Riesgo – DEST-Política-001, versión 2 del 14/04/2021.** Establece los lineamientos institucionales para la gestión del riesgo, roles de las líneas de defensa y responsabilidad de la Subdirección de Sistemas de Información en la gestión de riesgos de seguridad de la información.
- **Procedimiento para la Administración de Riesgos de Seguridad de la información - DEST–P-011, versión 1 del 19/09/2024.** Es el documento base que define las etapas de identificación, análisis, valoración y tratamiento de riesgos, incluyendo metodología de clasificación, criterio de aceptación y evaluación de controles.
- Se encuentra conforme a estándares internacionales, está alineado con la ISO/IEC 27001:2022 lo cual garantiza un enfoque estructurado, iterativo y documentado para la evaluación y tratamiento de riesgos.
- **El Instructivo para la Identificación y Valoración de Riesgos de Seguridad de la Información y valoración de controles existentes - DEST-I-004, versión1 del 19/09/2024.** Describe en detalle el proceso de aplicación de criterios de Confidencialidad, Integridad y Disponibilidad, métodos de valoración, clasificación de activos, construcción del mapa de riesgos y ejemplos de riesgos comunes en la ANT.
- **La forma DEST-F- 004 Mapa de Riesgos de la Seguridad de la Información, versión 2 del 3 febrero de 2025.** Evidencia la aplicación práctica del procedimiento, incluyendo clasificación

de activos de información por su por su criticidad (alta, media, baja), valoración por proceso, asignación de responsables y acciones de mejora.
- En cuanto a la valoración con criterios definidos, la ANT implementa una metodología de análisis y valoración de riesgos con criterios claros de probabilidad, impacto y nivel de exposición.

Así mismo, se evidenció Integración con el modelo de gestión institucional ya que el enfoque de gestión del riesgo está articulado con el Modelo Integrado de Planeación y Gestión (MIPG) y el Manual Estándar de Control Interno – MECI, lo que evidencia una integración formal con la estructura organizacional y de control interno de la entidad.
Para la evaluación de riesgos residuales y niveles de aceptación, se especifica que solo se aceptan riesgos residuales con nivel de exposición "Bajo", y que todos los riesgos deben contar con un plan de tratamiento a menos que se justifique su aceptación.

Adicionalmente, dentro de los mecanismos de seguimiento y mejora continua, se contempla una etapa formal de seguimiento, revisión y reporte, con participación de la Oficina de Planeación, Subdirección de Sistemas de Información y la Oficina de Control Interno, lo que garantiza la trazabilidad y la mejora continua del proceso.

Se concluye que la Agencia Nacional de Tierras cumple satisfactoriamente con el numeral 7.3.2 del MSPI, al disponer de un sistema integral, normativo y operativo para la valoración de los riesgos de seguridad de la información, alineado con estándares internacionales como ISO/IEC 27001:2022, el Modelo Estándar de Control Interno – MECI, y los lineamientos de la Función Pública puesto que**:**

- Existencia de metodología formal y aprobada.
- Aplicación de criterios cuantificables (probabilidad, impacto, nivel de riesgo residual).
- Registro y trazabilidad de los riesgos identificados.
- Articulación con los objetivos estratégicos y de proceso.
- Evaluación de efectividad de los controles existentes.
- Enfoque iterativo y mejora continua.
- Acompañamiento por parte de la Subdirección de Sistemas de Información y la Oficina de Planeación.

3.1.7. CONFORMIDAD Nro. 7. Disponibilidad y suficiencia de recursos para el MSPI.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI). Numeral 7.4.1.** Recursos.

CONDICIÓN OBSERVADA:

En la verificación realizada sobre el numeral 7.4.1 del Documento Maestro del MSPI y conforme a la lista de chequeo aplicada, se determinó que la entidad cumple en cuanto a la disposición de recursos financieros, humanos, tecnológicos y de gestión necesarios para la adopción, implementación, mantenimiento y mejora continua del modelo, asegurando con ello la sostenibilidad operativa y la articulación con la planeación institucional.

ANÁLISIS:

A continuación, se presenta los resultados conforme a la lista de chequeo aplicada:

- **Definición de recursos**

Se identificaron recursos asociados al MSPI en diversos instrumentos de planeación institucional, incluyendo el Plan de Acción 2025, el Plan de Gestión de Seguridad, el Plan de Tratamiento de Riesgos y la Cadena de Valor del proyecto Fortalecimiento de las soluciones tecnológicas para la transformación digital de los procesos institucionales a nivel nacional.

La verificación documental y la confirmación de la SSIT permitieron establecer que este proyecto contiene actividades directamente vinculadas al MSPI, tales como la implementación de controles de seguridad y privacidad de la información, el fortalecimiento de la gestión de información y el desarrollo de soluciones tecnológicas. Con ello, se demostró que la entidad definió formalmente recursos financieros, humanos, tecnológicos y de gestión para el modelo.

- **Disponibilidad de recursos financieros**

Se comprobó la existencia de proyectos de inversión aprobados y en ejecución con asignaciones específicas al MSPI:

- $12.095.038.212 en 2024
- $3.225.112.312 en 2025

Estos montos corresponden al proyecto *Fortalecimiento de las soluciones tecnológicas para la transformación digital de los procesos institucionales a nivel nacional*, que contempla la adquisición de firewalls, la operación de NOC/SOC y DRP, el licenciamiento Bitdefender y la vinculación de recurso humano.

El Plan de Acción 2025 y sus planes integrales (Gestión de Seguridad y Tratamiento de Riesgos) complementan esta trazabilidad, asegurando que las actividades del MSPI hacen parte de la planeación institucional. No se identificaron rubros de funcionamiento específicos, lo cual fue confirmado por la SSIT.

- **Recursos humanos**

La entidad dispone de personal contratado con dedicación total al MSPI durante 2024 y 2025, evidenciado en contratos de prestación de servicios que abarcan ciberseguridad, gestión de riesgos y tecnologías de la información. Adicionalmente, mediante la Resolución 202361002101356 de 2023 se designó a la Subdirectora de la SSIT como Oficial de Seguridad de la Información y de Protección de Datos Personales.

Si bien el equipo técnico del MSPI existe y opera en la práctica, aún falta la formalización del equipo humano coordinador ante el CIGD, lo que constituye un aspecto pendiente relacionado con el ítem 6 de roles y responsabilidades.

- **Recursos tecnológicos y de apoyo**

Se verificó la existencia de herramientas tecnológicas críticas contratadas en las vigencias 2024 y 2025, que garantizan las capacidades de prevención, detección, monitoreo y continuidad requeridas por el MSPI. Entre ellas se destacan:

- $6.231.995.000 – Firewall (2024)
- $5.279.735.385 – NOC/SOC y DRP (2024)
- $129.000.000 – Bitdefender (2024)
- $2.677.700.375 – NOC/SOC (2025)

Estas soluciones cuentan con soporte y periodos de vigencia que aseguran continuidad operativa más allá de un solo año.

- **Suficiencia de recursos**

Del análisis integral de los ítems anteriores se concluye que los recursos identificados y dispuestos permiten asegurar la adopción, implementación, mantenimiento y mejora continua del MSPI, al existir financiamiento específico, personal en funciones y soluciones tecnológicas críticas contratadas.

No obstante, se identificó como aspecto pendiente la formalización del equipo humano coordinador del MSPI por parte del CIGD, aspecto relevante para fortalecer la trazabilidad y gobernanza del modelo.

3.1.8. CONFORMIDAD Nro. 8. Cumplimiento en la formulación del Plan de tratamiento de los riesgos de seguridad de la información.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI). Numeral 7.3.3.** Plan de tratamiento de los riesgos de seguridad de la información.

- **INTI-Plan-005.** Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, versión 3 del 23/01/2025.

CONDICION OBSERVADA:

La Agencia Nacional de Tierras cuenta con los documentos **INTI-Plan-005** -Plan de Tratamiento de Riesgos 2025 versión v3 del 23/01/2025 aprobado por Comité Institucional de Gestión y Desempeño, Sesión 1 del 23 de enero de 2025.

ANALISIS:

De acuerdo con la revisión realizada por la Oficina de Control Interno respecto al cumplimiento del numeral 7.3.3 "Plan de tratamiento de los riesgos de seguridad de la información" del Modelo de Seguridad y Privacidad de la Información (MSPI), y teniendo en cuenta el Inventario de activos de información de la entidad así como el cumplimiento del numeral 7.3.2 "Valoración de los riesgos de seguridad de la información", se observó que la Agencia Nacional de Tierras (ANT) cuenta con un Plan de Tratamiento de Riesgos estructurado y documentado, el cual:

- Define objetivos generales y específicos alineados con los principios de confidencialidad, integridad y disponibilidad de la información.
- Establece acciones preventivas para mitigar los riesgos identificados.
- Tiene una metodología definida para la evaluación, análisis, monitoreo y seguimiento de riesgos.
- Incluye una Declaración de Aplicabilidad, basada en los 93 controles del Anexo A de la ISO/IEC 27001.

- Define un mapa de riesgos el cual contiene 117 acciones preventivas, y mecanismos de medición y verificación de controles.
- Está alineado con las políticas internas y estándares internacionales como ISO/IEC 27001 y las guías del DAFP y MinTIC.
- Contempla la implementación de controles sobre activos críticos de información previamente identificados y valorados.

Conforme con las evidencias anteriormente mencionadas, la Oficina de Control Interno concluye que la entidad cumple con los requisitos del numeral 7.3.3 3 del MSPI, al contar con un plan documentado, trazable, implementado y en ejecución, orientado a tratar los riesgos identificados sobre la seguridad de la información.

3.1.9. CONFORMIDAD Nro. 9. Cumplimiento del requisito de auditoría interna del MSPI con planificación y aprobación formal.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI). Numeral 9.1.2.** Auditoría Interna.

CONDICIÓN OBSERVADA:

La entidad cuenta con un programa de auditoría interna al MSPI en ejecución, conforme al Programa SEYM-F-005 V2, cuyo cronograma establece la entrega del informe final para el 2 de septiembre de 2025. El Plan Anual de Auditoría 2025 fue aprobado en sesión del Comité Institucional de Coordinación de Control Interno el 17 de marzo de 2025, incluyendo de manera explícita la revisión del MSPI. Esto demuestra que la organización dispone de la planificación y aprobación formal necesarias para la realización de auditorías internas en materia de seguridad y privacidad de la información, en concordancia con lo dispuesto en el numeral 9.1.2 del Documento Maestro del MSPI.

ANÁLISIS:

- **Resultados de auditorías internas**: La auditoría al MSPI se encuentra en curso, con levantamiento de información programado entre mayo y agosto de 2025, y con entrega del informe final prevista para septiembre. Aunque los resultados aún no están disponibles, el cronograma permite anticipar su cumplimiento dentro de los plazos establecidos.

- **No conformidades de auditorías internas**: La identificación de hallazgos y no conformidades será reportada en el informe preliminar del 26 de agosto y consolidada en el informe final del 2 de septiembre. A la fecha de verificación no existen hallazgos documentados, lo cual corresponde con el estado de ejecución del programa.
- **Plan de auditoría aprobado**: Se constató la aprobación del Plan Anual de Auditoría 2025 por parte del Comité Institucional de Coordinación de Control Interno, en cumplimiento del requisito normativo. Dicho plan contempla de manera expresa la auditoría al MSPI, en coherencia con los principios de trazabilidad y gobernanza del MECI y el MIPG.

Se concluye el cumplimiento del numeral 9.1.2 del Documento Maestro del MSPI en lo relacionado con la existencia de un programa de auditoría aprobado, en ejecución y con alcance sobre seguridad y privacidad de la información. El proceso avanza conforme a lo previsto, con informe final planificado para septiembre de 2025, lo que asegura que la evaluación de este componente se realice de manera formal y alineada con los lineamientos establecidos.

3.2. REQUISITOS CON INCUMPLIMIENTOS – NO CONFORMIDADES

3.2.1. NO CONFORMIDAD Nro. 1. Debilidades en el avance de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

CRITERIO:

- **Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información**.

5. Desarrollo de la metodología de autodiagnóstico.
5.1. Hoja 1 Portada.

CONDICIÓN OBSERVADA:

Se observaron debilidades en el avance de la implementación del MSPI, reflejadas en una cobertura limitada de procesos, un bajo desarrollo en las fases del ciclo PHVA y un nivel de madurez reducido. Esta situación contraviene lo definido en el *Instructivo para el Diligenciamiento de la Herramienta de Diagnóstico del MSPI* (MinTIC, 2017), el cual establece que las entidades deben evidenciar avances progresivos en el ciclo PHVA de acuerdo con los objetivos anuales de implementación del Manual de Gobierno en Línea, en concordancia con lo dispuesto en el Decreto 1078 de 2015, Título 9, Capítulo 1, Sección 3. Lo observado podría aumentar la exposición a incidentes de seguridad de la información,

comprometer la protección de los activos institucionales, afectar la continuidad operativa y limitar el cumplimiento progresivo de los lineamientos normativos aplicables.

La condición observada podría estar asociada a una planeación insuficiente del MSPI, que no contempló acciones progresivas para todas las fases del ciclo PHVA, sumada a la cobertura parcial de procesos, lo que limitó la aplicación del modelo en toda la entidad. Asimismo, se evidencian debilidades en el seguimiento institucional por la ausencia de revisiones periódicas, una marcada dependencia operativa de la SSIT sin suficiente acompañamiento estratégico del nivel directivo, y una articulación incompleta con la planeación institucional, factores que en conjunto explican el bajo nivel de madurez alcanzado en la implementación del modelo.

ANÁLISIS:

El autodiagnóstico en la Agencia se aplicó formalmente y muestra ligeros avances entre 2023 y 2024 (29% a 31%), pero el nivel de madurez se mantiene limitado. El autodiagnóstico realizado en 2024 muestra debilidades en el avance de la implementación del MSPI que se reflejan en tres aspectos principales: cobertura limitada de procesos, bajo desarrollo del ciclo PHVA y un nivel de madurez insuficiente, como se detalla a continuación:

- **Cobertura de procesos**

En la hoja “Levantamiento de información” se consigna lo siguiente:

- **Total de procesos:** 16.
- **Procesos definidos en el alcance MSPI:** 4.
- **Total, de avance por procesos:** 0,25 (25%).

Esto indica que el MSPI solo cubre una cuarta parte de los procesos institucionales. La baja cobertura demuestra que el modelo aún no se ha desplegado de manera integral en la entidad, lo cual limita su aplicación transversal y restringe la eficacia del ciclo PHVA.

- **Desarrollo del ciclo PHVA**

En la hoja “PHVA“se identifican los siguientes resultados:

- **Planificación:** promedio bajo, con algunos avances parciales.
- **Implementación:** avances limitados.
- **Evaluación del desempeño:** desarrollo muy reducido.
- **Mejora continua:** desarrollo muy reducido.

Los resultados muestran un desarrollo insuficiente en todas las fases, especialmente en Implementación, Evaluación y Mejora. Si bien se han adelantado algunas acciones en Planificación, estas no son suficientes para cerrar el ciclo de gestión ni para alcanzar un nivel adecuado de madurez.

- **Nivel de madurez**

El autodiagnóstico refleja que la Agencia presenta un nivel de madurez limitado, con avances puntuales, pero sin consolidar plenamente ninguno de los niveles definidos.

- En el nivel inicial (1), varios requisitos fueron calificados como “suficiente”, lo que muestra que la entidad ha adoptado algunas prácticas básicas del MSPI, aunque no de manera integral.
- En el nivel repetible (2), algunos requisitos fueron calificados como “intermedio”, lo que refleja esfuerzos incipientes hacia la sistematización de prácticas de seguridad. Sin embargo, otros criterios permanecen en estado “menor”, lo que impide alcanzar este nivel.

La coexistencia de valoraciones **“**suficiente” en el nivel inicial y “intermedio” en el nivel 2 muestra avances parciales, pero la falta de homogeneidad y la permanencia de debilidades hacen que el modelo no pueda reconocerse formalmente ni en el nivel 1 ni en el nivel 2. En consecuencia, el resultado global es de madurez limitada, en estado de transición, insuficiente frente a los objetivos definidos en el Instructivo MSPI (MinTIC, 2017) y el Manual de Gobierno Digital.

- **Recursos invertidos en contratistas**

De manera complementaria, se identificó que la entidad ha destinado recursos económicos a la contratación de personal de apoyo en seguridad de la información y en actividades asociadas al MSPI. Sin embargo, los resultados del autodiagnóstico muestran que, pese a esta inversión, los avances en cobertura de procesos, desarrollo del ciclo PHVA y nivel de madurez permanecen limitados. Los registros de contratación evidencian lo siguiente:

Vigencia	Total Contratos	Valor Total
2024	11	$454.307.827
2025	7	$547.411.937
Total	**18**	**$1.001.719.764**

Tabla 1. *Contratos implementación MSPI.*
Fuente: *Correo electrónico SSJ del 25/08/2025.*

OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025.

"Frente a la No Conformidad No1 Debilidades en el avance de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI); nos permitimos realizar las siguientes precisiones:

*Frente a lo expuesto: (…) se evidencian **debilidades en el seguimiento institucional** por **la ausencia de revisiones periódicas, una marcada dependencia operativa de la SSIT sin suficiente acompañamiento estratégico del nivel directivo, y una articulación incompleta con la planeación institucional,** factores que en conjunto explican el bajo nivel de madurez alcanzado en la implementación del modelo.*

Con respecto a la afirmación sobre la supuesta ausencia de revisiones periódicas y la falta de acompañamiento estratégico del nivel directivo en la implementación del MSPI, me permito aclarar lo siguiente:

- ***Participación de la Alta Dirección***

El Modelo de Seguridad y Privacidad de la Información – MSPI ha sido presentado en el Comité Institucional de Gestión y Desempeño, en donde participa de manera integral la Alta Dirección. En estos escenarios se han socializado los avances, resultados y retos del modelo, evidenciando un acompañamiento estratégico y un compromiso directivo con la implementación. Soportes presentados en la etapa de "Solicitud de Información"

- ***Revisiones periódicas***

A lo largo de la vigencia 2024–2025 se han realizado presentaciones periódicas de avances y seguimiento al MSPI, así como la integración de indicadores dentro de los planes institucionales, lo cual permite monitorear su evolución y generar acciones de mejora continua. Soportes presentados en la etapa de "Solicitud de Información"

- ***Alineación con la planeación institucional***

*El MSPI se encuentra articulado con el **Plan de Acción Institucional** y con el **PETI**, donde se incluyen actividades específicas relacionadas con gestión de riesgos, gestión de incidentes, y adquisición de herramientas tecnológicas. Lo anterior demuestra que la gestión de seguridad no se limita a la SSIT, sino que hace parte de la estrategia institucional. Soportes presentados en la etapa de "Solicitud de Información"*

Por lo anterior solicitamos revisar los expuesto en el párrafo.

Frente al análisis me permito exponer lo siguiente:

*Por otro lado es importante precisar que el autodiagnóstico citado corresponde a la información consolidada **con corte a noviembre de 2024**. Por lo tanto, los resultados allí reflejados no incorporan las acciones desarrolladas durante la vigencia 2025, tanto en términos de **implementación operativa** como de **recursos asignados**, que han fortalecido el nivel de madurez del MSPI.*
*Así mismo, se debe aclarar que la **implementación formal del modelo inició a finales de 2023**, razón por la cual el periodo evaluado corresponde a una fase temprana de despliegue. En consecuencia, los resultados del diagnóstico deben interpretarse como una **línea base inicial** y no como el reflejo de la consolidación total del modelo.*

Adicionalmente, se considera necesario precisar que, en los instrumentos del MinTIC, ***no se establece un porcentaje de avance esperado por año*** *ni una tasa mínima de crecimiento del nivel de madurez del MSPI. Lo que se plantea en dichos lineamientos es un proceso* ***progresivo, flexible y contextualizado****, que depende de la naturaleza, recursos y prioridades de cada entidad.*
Por lo anterior, la comparación entre los recursos invertidos y el nivel de avance no debe interpretarse de manera lineal ni exclusivamente cuantitativa, dado que el fortalecimiento de capacidades en seguridad de la información requiere tiempo, maduración institucional y un despliegue gradual a través de todas las fases del ciclo PHVA.

Frente a la cobertura de procesos: estrategia de implementación progresiva
La cobertura del 25% de los procesos institucionales responde a una ***estrategia de priorización técnica****, en la que se han abordado inicialmente los procesos misionales y críticos que gestionan información sensible. Esta decisión está alineada con las buenas prácticas de gestión de riesgos y permite focalizar recursos en áreas de mayor impacto. La ampliación de cobertura está contemplada en el Plan de Cierre de Brechas y será ejecutada en fases posteriores. De igual forma es pertinente mencionar que la identificación de riesgos y el inventario de activos, como parte integral del proceso, evidencian la amplitud del alcance y la aplicación de la gestión de seguridad de la información en todas las dependencias y procesos.*

Nivel de madurez: transición entre niveles 1 y 2
El autodiagnóstico refleja una ***transición entre los niveles de madurez 1 (inicial) y 2 (repetible)****. La coexistencia de valoraciones "suficiente" e "intermedio" demuestra que la entidad ha superado la etapa de adopción básica y se encuentra en proceso de sistematización. Este estado* ***es coherente con el tiempo de implementación del modelo*** *y con el enfoque gradual recomendado por el MinTIC*

<u>Conclusión SSIT</u>

En consideración a lo expuesto, estimamos que los aspectos señalados corresponden ***a oportunidades de fortalecimiento técnico e institucional****, que ya se encuentran siendo abordadas mediante acciones estructuradas, más que a una* ***No Conformidad propiamente dicha****.*
La ISO/IEC 27001:2022*, en su numeral* ***9.3 – Revisión por la Dirección****, establece que el seguimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI) deben realizarse de manera periódica, flexible y progresiva, en coherencia con el contexto y los recursos de cada organización. En este sentido, la ANT ha demostrado avances en la implementación del MSPI mediante revisiones periódicas, participación de la Alta Dirección y alineación con la planeación institucional, lo que evidencia cumplimiento con los criterios normativos.*

Adicionalmente, la norma dispone que la gestión del SGSI debe desarrollarse bajo el ***ciclo PHVA (Planear, Hacer, Verificar, Actuar),*** *lo que implica que la madurez del modelo se consolida de manera gradual, a través de fases sucesivas de mejora continua. Bajo este enfoque, los resultados obtenidos*

constituyen un estado de transición entre niveles de madurez, coherente con el tiempo de implementación del MSPI y con las recomendaciones metodológicas del MinTIC.

Por lo anterior, solicitamos respetuosamente a la Oficina de Control Interno reconsiderar la calificación del hallazgo y ajustarlo a "Oportunidad de Mejora", de forma que refleje el contexto real de implementación y la evidencia actualizada del MSPI, en concordancia con los lineamientos de la Norma ISO/IEC 27001:2022 y con el principio de mejora continua que orienta su aplicación."

CONCLUSIÓN EQUIPO AUDITOR

En atención a la observación presentada por la SSIT frente a la No Conformidad Nro. 1 Debilidades en el avance de la implementación del MSPI, se precisa que el hallazgo se fundamentó en el incumplimiento de lo dispuesto en el Instructivo para el Diligenciamiento de la Herramienta de Diagnóstico del MSPI (MinTIC, 2017), el cual establecen la obligación de evidenciar avances progresivos en el ciclo PHVA conforme a los objetivos anuales definidos en el Manual de Gobierno en Línea. El autodiagnóstico reportó avances del 29% en 2023 y 31% en 2024, valores que no alcanzan los porcentajes de referencia señalados en dichos lineamientos. Las causas mencionadas en el informe constituyen únicamente posibles factores asociados a la condición observada, siendo responsabilidad de la dependencia competente realizar el análisis de causa raíz y definir el plan de mejoramiento correspondiente. En este sentido, al verificarse un incumplimiento frente a un requisito obligatorio, el hallazgo se clasifica como No Conformidad, diferenciándose de una *Oportunidad de Mejora*, aplicable únicamente cuando no existe contravención directa de los criterios de auditoría.

En consecuencia, se mantiene la No Conformidad Nro. 1, toda vez que el MSPI de la Agencia no cumple con los avances progresivos requeridos en el ciclo PHVA, de acuerdo con lo definido normativamente.

3.2.2. NO CONFORMIDAD Nro. 2. Debilidades en la definición específica del contexto de la entidad conforme al MSPI.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI). Numeral. 7.1.1.** Comprensión de la organización y de su contexto.

CONDICIÓN OBSERVADA:

Se evidenció que la Agencia Nacional de Tierras ha desarrollado un análisis general de su entorno institucional y misión estratégica.

Se observó que en Manual INTI-M-001-Sistema de Gestión de Seguridad de la Información v1 30/12/2024 se encuentra el ítem 6.1. Contexto interno y Externo **“** La Agencia Nacional de tierras es una entidad pública que como lo establece el decreto 2363 de 2015 “es la máxima autoridad de las tierras de la Nación y tendrá por objeto ejecutar la política de ordenamiento social de la propiedad rural formulada por el Ministerio de Agricultura y Desarrollo Rural, para lo cual deberá gestionar el acceso tierra como factor productivo, lograr la seguridad jurídica sobre ésta, promover su uso en cumplimiento de la función social de la propiedad y administrar y disponer de los predios rurales de propiedad de la Nación”

ANALISIS:

En cuanto al cumplimiento del ítem 7.1.1 Comprensión de la organización y de su contexto**,** se evidenció la necesidad de que la entidad incorpore de manera integral los lineamientos establecidos en el Manual Operativo del Modelo Integrado de Planeación y Gestión (MIPG). Particularmente, se identificó que la ANT debe asegurar la articulación efectiva de su modelo estratégico, modelo de procesos, modelo de servicios y modelo organizacional, conforme al Marco de Referencia de Arquitectura Empresarial definido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). La integración de estos modelos es esencial para garantizar la coherencia entre la planeación institucional, la gestión operativa y la prestación de servicios, así como para fortalecer la capacidad institucional y la generación de valor público, en concordancia con los principios de gestión del MIPG teniendo en cuenta los siguientes criterios**:**

- Ley 1753 de 2015 – Plan Nacional de Desarrollo.
- Decreto 1499 de 2017 – Por el cual se actualiza el MIPG.
- Manual Operativo del Modelo Integrado de Planeación y Gestión (MIPG).
- Marco de Referencia de Arquitectura Empresarial – MinTIC.

Donde la falta de alineación y articulación explícita entre los modelos internos de la entidad y los marcos de referencia definidos por MinTIC, el Manual Operativo del MIPG pueden ocasionar posibles incoherencias entre la planeación estratégica, los procesos misionales y el modelo de servicios institucional, lo que puede impactar la eficiencia en la gestión y la generación de valor público, refiriéndose al conjunto de beneficios tangibles e intangibles que la entidad genera para la ciudadanía y los grupos de interés, mediante la protección eficaz de la información, en aspectos como confidencialidad, integridad, disponibilidad y trazabilidad.

Adicionalmente, la Generación de valor público a través de la seguridad de la información se debe tener en cuenta como la gestión adecuada de la seguridad de la información en la Agencia Nacional de Tierras (ANT) lo cual constituye un elemento fundamental para la generación de valor público, en tanto que fortalece la confianza de los ciudadanos, usuarios y grupos de interés en los servicios que presta la entidad. Al garantizar la confidencialidad, integridad y disponibilidad de la información institucional especialmente aquella relacionada con derechos sobre la tierra, procesos administrativos, bases de datos geográficas y catastros se mitigan riesgos de corrupción, pérdida de información, manipulación indebida y fallas en la prestación de servicios.

La implementación de controles robustos en seguridad de la información no solo asegura el cumplimiento normativo (Ley 1581 de 2012, Decreto 1377 de 2013, Decreto 1081 de 2015, y el Modelo de Seguridad y Privacidad de la Información del MinTIC), sino que también facilita la transparencia, la equidad en el acceso a los servicios públicos, y la mejora en la experiencia del ciudadano. En este sentido, la seguridad de la información se convierte en un habilitador estratégico para la consolidación de una administración pública digital, confiable y orientada a resultados.

La Oficina de Control Interno identificó la ausencia de un análisis formal, estructurado y documentado del contexto institucional desde el enfoque de seguridad de la información, lo que evidencia una debilidad frente al cumplimiento del numeral 7.1.1 del Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI).

Esta condición limita la capacidad de la Agencia Nacional de Tierras para identificar con precisión los factores internos y externos que afectan el cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI), debilitando así su planeación estratégica, su capacidad de prevención frente a incidentes y su ciclo de mejora continua.

No se evidencian de manera clara y documentada las cuestiones internas y externas que impactan directamente el SGSI, ni su vinculación con el diagnóstico del MSPI, la gestión de riesgos o el diseño de controles. Ya que, hacer el contexto es un proceso integral que asegura que el modelo esté bien fundamentado y alineado con las realidades y objetivos de la entidad, proporcionando una guía clara para la implementación y mejora continua de la seguridad y privacidad de la información.

En cuanto al contexto externo, se cumple parcialmente, ya que se hace mención del Decreto 2363 de 2015 y al rol institucional de la ANT, lo cual es pertinente. Sin embargo, respecto al contexto interno (estructura organizacional, recursos tecnológicos, procesos críticos, cultura organizacional y capacidades disponibles), no se encuentran referencias específicas ni análisis detallado que permitan comprender cómo estos elementos afectan o condicionan la seguridad de la información.

Tampoco se observa desarrollado el vínculo entre el análisis de contexto y los riesgos, oportunidades o requisitos aplicables al SGSI, ni se evidencia que dicho análisis haya servido como insumo para la planificación del MSPI ni para el diseño e implementación de controles de seguridad.

Así mismo, la ANT debe asegurar que su modelo estratégico, de procesos, organizacional y de servicios se encuentren alineados con el Marco de Referencia de Arquitectura Empresarial definido por el MinTIC, de forma que se garantice una gestión integrada y segura de la información a lo largo del ciclo de vida institucional.

La incorporación del MSPI en este contexto permite a la entidad establecer políticas, procedimientos, roles, tecnologías y controles que aseguren la confidencialidad, integridad, disponibilidad, trazabilidad y privacidad de la información, contribuyendo así a la generación de valor público, al fortalecimiento de la confianza institucional y al cumplimiento del marco legal vigente.

OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025.

"Frente al criterio y al análisis realizado me permito mencionar lo siguiente:

Con relación al documento INTI-M-001 - Manual del Sistema de Gestión de Seguridad de la Información, numerales 6.1 Contexto interno y externo y 6.2 Comprensión de las necesidades y expectativas, expongo las siguientes consideraciones:

- *La ANT sí realizó un análisis de contexto, incluyendo factores internos y externos, así como el uso de herramientas como FODA, PESTEL y el Mapa de Riesgos de Seguridad de la Información. Por tanto, el requisito no está ausente en el SGSI.*
- *Si bien se reconoce que el análisis de contexto del SGSI puede fortalecerse en su articulación con la gestión de riesgos, oportunidades y controles del MSPI, se debe precisar que la Agencia ya cuenta con un contexto documentado y vigente.*
- *En este sentido, lo señalado corresponde más a una oportunidad de mejora que a una no conformidad, toda vez que el requisito establecido en el numeral 7.1.1 del Documento Maestro del MSPI no se encuentra incumplido, sino que requiere un mayor nivel de integración con los lineamientos de MIPG y MinTIC.*

Conclusión SSIT

*Por lo anterior, respetuosamente solicito que la presente observación sea reconsiderada y reclasificada como una **oportunidad de mejora**, y no como una **No Conformidad**, toda vez que la **ISO/IEC 27001:2022, en sus numerales 4.1 – Comprensión de la organización y de su contexto y 4.2 – Comprensión de las necesidades y expectativas de las partes interesadas**, exige la identificación y*

análisis de factores internos, externos y expectativas, requisito que la ANT ya cumple mediante la aplicación de metodologías como FODA, PESTEL y el Mapa de Riesgos de Seguridad de la Información.

*Si bien se reconoce la necesidad de fortalecer la integración de dicho análisis con la gestión de riesgos, oportunidades y controles del MSPI, este aspecto no constituye un incumplimiento normativo, sino un elemento perfectible en el marco de la mejora continua del SGSI. En consecuencia, lo señalado corresponde a **una oportunidad de mejora**, en concordancia con lo establecido en el **numeral 7.1.1 del Documento Maestro del MSPI** y los lineamientos de MIPG y MinTIC.".*

CONCLUSIÓN EQUIPO AUDITOR

La Oficina de Control Interno, tal como se señala en el análisis de la No Conformidad, identificó ejercicios previos de análisis de contexto realizados por la ANT; sin embargo, a partir de su revisión concluyó que estos presentan debilidades frente a lo requerido en el numeral 7.1.1 del Documento Maestro del MSPI, toda vez que no se evidenció un análisis integral y articulado que vincule el contexto institucional con la planeación estratégica, la gestión de riesgos, los controles y los modelos organizacionales. Esta situación constituye un incumplimiento que limita la capacidad de la entidad para garantizar coherencia, trazabilidad y generación de valor público en el SGSI. Donde las posibles causas pueden ser un enfoque parcial en la recopilación y análisis de información, debilidades metodológicas en la aplicación de la guía establecida, falta de articulación entre dependencias responsables y la escasa revisión de calidad y trazabilidad en los documentos elaborados. Por lo anterior, y pese a las observaciones de la SSIT, se mantiene la No Conformidad Nro. 2.

Cabe precisar que un hallazgo de tipo No Conformidad se presenta cuando existe un incumplimiento verificable frente a un requisito normativo, lo cual exige la implementación de acciones de mejora. En contraste, una Oportunidad de Mejora corresponde a hallazgos de tipo conforme que no constituyen incumplimiento de los criterios normativos, pero que evidencian posibilidades de optimizar la eficiencia, eficacia o control en los procesos.

3.2.3. NO CONFORMIDAD Nro. 3. Debilidades en la determinación de partes interesadas relevantes para la Seguridad de la Información.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI). Numeral. 7.1.2.** Necesidades y expectativas de los interesados.

CONDICION OBSERVADA:

La Agencia Nacional de Tierras (ANT), en su rol de autoridad encargada de gestionar el acceso, uso y formalización de la propiedad rural en Colombia, interactúa con diversas partes interesadas que tienen necesidades, expectativas y obligaciones específicas respecto a la seguridad y privacidad de la información.

Se observó que en Manual INTI-M-001-Sistema de Gestión de Seguridad de la Información v1 30/12/2024 se encuentra el ítem 6.2**.** Comprensión de las necesidades y expectativas donde se indica "A fin de identificar y comprender las necesidades y expectativas de sus partes interesadas, la Agencia Nacional de Tierras aplica la política de participación ciudadana y ejecuta las actividades de gestión para la transparencia y direccionamiento del servicio al ciudadano del proceso de comunicación y gestión con grupos de interés. Sumado a esto se identifican las partes interesadas con el objetivo de mantener actualizada la información y dar cumplimiento a los requerimientos de las mismas".

ANALISIS:

La Agencia Nacional de Tierras debe determinar las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información y sus requisitos pertinentes

Se evidenció *Tabla 1. Grupos de Interés Agencia Nacional de Tierras* en el Manual INTI-M-001-Sistema de Gestión de Seguridad de la Información v1 30/12/2024 ítem 6.2. Comprensión de las necesidades y expectativas.

No se evidencian criterios de análisis específicos desde el enfoque de seguridad de la información.
El texto es general y no vincula explícitamente las necesidades y expectativas identificadas con la seguridad de la información (confidencialidad, integridad, disponibilidad).

No se observa una matriz de partes interesadas formal y trazable dentro del SGSI o del MSPI que permita su actualización y que tenga una identificación para el sistema. Tampoco se encontraron registros que evidencien el análisis de sus necesidades y expectativas en materia de seguridad de la información.

No queda claro si las partes interesadas han sido categorizadas, ni si se han definido requisitos pertinentes de seguridad (por ejemplo, entes de control, ciudadanía, proveedores tecnológicos, usuarios internos, etc.).

El numeral 7.1.2 Necesidades y expectativas de los interesados exige que la organización determine cuáles de esas necesidades se vuelven obligatorias para el SGSI. Esa decisión no está documentada en lo observado.

Igualmente, no se identificó que la entidad haya determinado de manera explícita cuáles de estas necesidades se constituyen en requisitos aplicables para la planeación, implementación y mantenimiento del SGSI.

La ANT debe reconocer y gestionar adecuadamente estas expectativas es clave para fortalecer la confianza pública, garantizar la legalidad y lograr una operación eficiente y transparente para lo cual debe tener en cuenta:

- Parte interesada
- Rol / Relación con la ANT
- Necesidades / Expectativas
- Impacto en el SGSI (Alto, Medio o bajo)

La Oficina de Control Interno evidenció que la Agencia Nacional de Tierras no cuenta con una identificación formal, actualizada y documentada de las partes interesadas relevantes para el sistema de Seguridad de la Información. Tampoco se encontraron registros que evidencien el análisis de sus necesidades y expectativas en materia de seguridad de la información.

OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025.

"Frente al análisis realizado en relación con el numeral 7.1.2 del MSPI, me permito manifestar lo siguiente:

1. La ANT sí cuenta con la identificación de las partes interesadas en el documento INTI-M-001 – Manual del Sistema de Gestión de Seguridad de la Información, específicamente en el numeral 6.2 Comprensión de las necesidades y expectativas y en la Tabla 1, donde se encuentran relacionadas las partes interesadas y su interacción con la Entidad.

2. Es importante precisar que el requisito no se encuentra ausente, ya que se tiene evidencia documental del análisis y de la gestión institucional que la Agencia realiza con los grupos de interés a través de los mecanismos de participación, transparencia y rendición de cuentas.

3. Se reconoce que el análisis existente puede fortalecerse en su articulación con los aspectos específicos de seguridad de la información (confidencialidad, integridad y disponibilidad), así como en la construcción de una matriz formal que permita establecer una mayor trazabilidad entre partes interesadas, necesidades, expectativas y requisitos obligatorios.

4. En este sentido, lo identificado corresponde más a una oportunidad de mejora que a una no conformidad, toda vez que el requisito establecido en el MSPI sí está documentado y en ejecución,

aunque requiere mayor nivel de madurez e integración para dar cumplimiento pleno a los lineamientos de MIPG y MinTIC.

Conclusión SSIT

Respetuosamente solicitamos que la observación sea reconsiderada y reclasificada como una Oportunidad de Mejora, en la medida en que la ANT sí da cumplimiento al requisito establecido en la ISO/IEC 27001:2022, numeral 4.2 – Comprensión de las necesidades y expectativas de las partes interesadas, el cual se encuentra documentado en el Manual del SGSI (INTI-M-001). Lo identificado corresponde a un aspecto perfectible de trazabilidad y articulación, y no a una No Conformidad."

CONCLUSIÓN EQUIPO AUDITOR

La Oficina de Control Interno reconoce que la ANT cuenta con una identificación general de partes interesadas en el Manual del SGSI (numeral 6.2 y Tabla 1). Sin embargo, se evidenció que dicha información no incorpora un análisis formal y específico desde el enfoque de seguridad de la información ni establece criterios claros de categorización, requisitos aplicables o trazabilidad frente al SGSI. La ausencia de una matriz estructurada y actualizada que vincule necesidades y expectativas con los principios de confidencialidad, integridad y disponibilidad limita la gestión efectiva del modelo y afecta el cumplimiento del numeral 7.1.2 del MSPI el cual exige que la organización identifique y gestione de manera estructurada las necesidades y expectativas de las partes interesadas vinculadas al SGSI.

La ausencia de un análisis formal y una matriz actualizada limita la capacidad de la entidad para gestionar de manera efectiva las expectativas de las partes interesadas, afecta la alineación con los principios de seguridad de la información y reduce la eficacia del SGSI en la generación de valor público y en la protección de los activos de información. Donde las posibles causas pueden ser un enfoque descriptivo y no analítico en la identificación de partes interesadas, falta de lineamientos metodológicos para categorizar y priorizar necesidades, limitada revisión periódica de la información documentada. Por lo anterior, y pese a las observaciones de la SSIT, se mantiene la No Conformidad Nro. 3

Cabe precisar que un hallazgo de tipo No Conformidad se presenta cuando existe un incumplimiento verificable frente a un requisito normativo, lo cual exige la implementación de acciones de mejora. En contraste, una Oportunidad de Mejora corresponde a hallazgos de tipo conforme que no constituyen incumplimiento de los criterios normativos, pero que evidencian posibilidades de optimizar la eficiencia, eficacia o control en los procesos.

3.2.4. NO CONFORMIDAD Nro. 4. Debilidades en la definición formal y aprobación del alcance del MSPI.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI). Numeral 7.1.3.** Definición del alcance del MSPI.

CONDICION OBSERVADA:

Durante la auditoría se evidenció que la Agencia Nacional de Tierras (ANT) no cuenta con un documento formal y específico que defina claramente el alcance del MSPI, de acuerdo con lo establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) en el Numeral 7.1.3. Definición del alcance del MSPI.

Se observó que en Manual INTI-M-001-Sistema de Gestión de Seguridad de la Información v1 30/12/2024 se encuentra el ítem 6.3. Alcance de la Gestión de la Seguridad de la información donde se indica “El sistema de gestión de seguridad de la información de la Agencia Nacional de Tierras se aplica a todos los procesos estratégicos, misionales, de apoyo y de evaluación y control en sus sedes y UGT a nivel nacional”.

ANÁLISIS:

Se define de forma general la aplicabilidad del SGSI a todos los procesos y niveles de la entidad, incluyendo procesos estratégicos, misionales, de apoyo, de control y cobertura territorial (sedes y UGT). El texto dentro del manual que indica el alcance, evidencia intención formal de cumplimiento del requisito.

Se define de forma general la aplicabilidad del SGSI a todos los procesos y niveles de la entidad, incluyendo procesos estratégicos, misionales, de apoyo, de control y cobertura territorial (sedes y UGT).

Sin embargo, aunque se identifican algunas referencias generales a la seguridad de la información en documentos de la Entidad, no se especifican los límites del SGSI de forma detallada, las ubicaciones físicas, los activos de información, procesos, sistemas o áreas organizativas que se encuentran dentro del alcance del Modelo, ni se justifica de manera técnica la exclusión de elementos fuera del mismo.

Tampoco se evidenció trazabilidad entre el alcance declarado y el contenido del diagnóstico de seguridad, la gestión de riesgos o los controles implementados. Esto limita la planificación, aplicación y seguimiento efectivo del SGSI y del MSPI en la entidad.

La Oficina de Control Interno conforme a la revisión de los documentos aportados por la SSIT tuvo en cuenta los siguientes criterios con respecto al ítem 7.1.3 del Documento Maestro del MSPI y la Resolución 500/2021 – Anexo 1:

Criterio de evaluación	Requisito normativo (MSPI)	Situación en la ANT
¿Se incluye en el alcance la información, procesos, servicios, infraestructura y sedes relevantes?	7.1.3 Definición del alcance del MSPI	No se evidencia un documento formal que lo contenga.
¿El alcance está alineado con el contexto de la organización y los riesgos identificados?	7.1.1 Comprensión de la organización y de su contexto 7.3.2 Valoración de los riesgos de seguridad de la información	No se evidencia un documento formal que demuestre el alcance y el contexto.
¿Se identifican y justifican exclusiones del alcance?	7.1.3 Definición del alcance del MSPI	No se identifican exclusiones explícitas ni existe documento que las justifique formalmente, la "definición del alcance" implica establecer con claridad los límites y aplicabilidad del Sistema de Gestión de Seguridad de la Información (SGSI) dentro de la entidad. Estas exclusiones deben estar claramente justificadas, documentadas y no deben comprometer la efectividad del sistema de gestión, ni dejar brechas significativas de seguridad.
¿Existe un documento formal que defina el alcance del MSPI o del SGSI en la ANT?	Resolución 500/2021 – Anexo 1 (componente 2.2)	Se evidencia que algunos elementos del alcance están identificados en planes o diagnósticos, pero no consolidado formalmente en un único documento aprobado y difundido.
¿El alcance ha sido aprobado y comunicado a las partes internas relevantes?	MIPG Política de Gestión	No se evidencian actas ni actos administrativos que apruebe y se difunda el alcance del MSPI a funcionarios.

Tabla 2. 2 *Alcance*
Fuente: *Creación propia*

La Agencia Nacional de Tierras no cumple completamente con los requisitos del numeral 7.1.3 del Documento Maestro del MSPI ni con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) definidos por MinTIC, en cuanto a la definición formal, documentada y aprobada del alcance del SGSI donde se debe tener en cuenta:

La elaboración y aprobación formal de un documento institucional que defina el alcance del MSPI, incluyendo:

- Procesos, áreas, información, sistemas, infraestructura, sedes, servicios y terceros involucrados.
- Justificación de cualquier exclusión.
- Relación con los riesgos identificados.
- Alineación del alcance con el contexto institucional y los elementos del modelo de arquitectura empresarial.
- Socializar el alcance a las áreas responsables y partes interesadas internas.
- Incluir el alcance en la política de seguridad de la información y mantenerlo disponible para auditorías y revisiones.

OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025.

"Si bien se reconoce que existen oportunidades de mejora en la formalización documental del alcance del SGSI, la Agencia Nacional de Tierras sí cumple con los requisitos sustanciales del numeral 7.1.3 del Documento Maestro del MSPI y con los lineamientos de MinTIC. La implementación técnica, operativa y estratégica del SGSI está en marcha, y se encuentra en proceso de fortalecimiento continuo conforme al ciclo PHVA."

CONCLUSIÓN EQUIPO AUDITOR

La Oficina de Control Interno observó la existencia de referencias generales al alcance en el Manual INTI-M-001; sin embargo, se concluye que la ANT no cuenta con un documento formal, específico y aprobado que defina de manera clara y trazable el alcance del MSPI, incluyendo los procesos, así como exclusiones justificadas. Tampoco se evidenció alineación entre el alcance, el diagnóstico, la gestión de riesgos ni los controles implementados, ni registros de aprobación y socialización interna. Esta situación constituye un incumplimiento frente al numeral 7.1.3 del Documento Maestro del MSPI el cual exige la definición formal, aprobada y documentada del alcance del modelo, en coherencia con la planeación y la gestión de riesgos limitando la planificación, implementación y seguimiento del SGSI. Donde las posibles causas son un enfoque parcial en la definición del alcance del modelo, ausencia

de lineamientos institucionales claros para documentar exclusiones y justificaciones, debilidades en los mecanismos de revisión, aprobación y socialización interna y falta de articulación entre responsables de planeación, riesgos y seguridad de la información. En consecuencia, y pese a las observaciones de la SSIT, se mantiene la No Conformidad Nro. 4.

Cabe precisar que un hallazgo de tipo No Conformidad se presenta cuando existe un incumplimiento verificable frente a un requisito normativo, lo cual exige la implementación de acciones de mejora. En contraste, una Oportunidad de Mejora corresponde a hallazgos de tipo conforme que no constituyen incumplimiento de los criterios normativos, pero que evidencian posibilidades de optimizar la eficiencia, eficacia o control en los procesos.

3.2.5. NO CONFORMIDAD Nro. 5. Debilidades en el liderazgo y compromiso del Comité Institucional de Gestión y Desempeño frente al MSPI.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI). Numeral 7.2.1.** Liderazgo y Compromiso.

- Garantizar la adopción de los requisitos del MSPI en los procesos de la entidad.
- Comunicar en la entidad la importancia del MSPI.
- Asegurar que, el MSPI consiga los resultados previstos.
- Realizar revisiones periódicas de la adopción del MSPI (mínimo dos veces por año con participación del nominador).
- Garantizar el liderazgo y compromiso del CIGD para alcanzar los objetivos de implementación del MSPI.

CONDICION OBSERVADA:

En la verificación realizada sobre el numeral 7.2.1 del Documento Maestro del MSPI, se determinó que la entidad no cumple integralmente con las funciones de liderazgo y compromiso asignadas al CIGD, específicamente en lo relacionado con: garantizar la adopción de los requisitos del modelo en los procesos de la entidad, comunicar su importancia a nivel institucional, asegurar que el MSPI consiga los resultados previstos, realizar revisiones periódicas de su adopción con la participación del nominador, y garantizar el liderazgo y compromiso del Comité para alcanzar los objetivos de implementación. Lo observado limita la gobernanza del modelo, reduce su cobertura en los procesos

institucionales, debilita la apropiación por parte de los funcionarios y aumenta el riesgo de no alcanzar los resultados previstos ni asegurar la sostenibilidad del sistema.

La condición observada podría estar asociada a la ausencia de priorización del MSPI en la agenda del CIGD, lo que ha limitado su discusión formal y el aval explícito en actas. Adicionalmente, se evidencia una dependencia operativa de la SSIT para la planeación y ejecución de actividades, sin que exista un acompañamiento estratégico consistente del Comité. Esto ha derivado en una cobertura parcial del modelo en los procesos institucionales, una débil articulación interdependencias para integrar el MSPI y la falta de mecanismos de seguimiento periódico definidos por el CIGD para evaluar avances, resultados y sostenibilidad del modelo.

ANALISIS:

- **Garantizar la adopción de los requisitos del MSPI en los procesos.**

El autodiagnóstico 2024 mostró que solo 4 de los 16 procesos institucionales (25%) han incorporado los requisitos del MSPI. Las actas de 2023 y 2024 no registran análisis ni decisiones estratégicas para extender la cobertura a los demás procesos. Esto evidencia que la adopción es parcial y no transversal a la entidad

- **Comunicar en la entidad la importancia del MSPI.**

Aunque existe un plan formal de comunicación y sensibilización, su ejecución presenta cobertura insuficiente (17,53% de los funcionarios) y carece de indicadores de impacto, mensajes segmentados y participación de actores externos. Adicionalmente, las actas del CIGD no reflejan un seguimiento estratégico de este aspecto, lo que limita la apropiación institucional del modelo.

- **Asegurar que el MSPI consiga los resultados previstos.**

El análisis del autodiagnóstico 2024 reflejó que el modelo no ha alcanzado los resultados esperados, ya que presenta cobertura restringida de procesos, avances limitados en las fases del ciclo PHVA y un nivel de madurez bajo. Esto impide consolidar una gestión integral y sostenible de la seguridad y privacidad de la información.

- **Realizar revisiones periódicas de la adopción del MSPI.**

Se identificó un único registro de socialización del autodiagnóstico en diciembre de 2024, lo que no cumple con la exigencia de realizar al menos dos revisiones anuales con participación del nominador. Esta situación limita la capacidad de seguimiento oportuno y la toma de decisiones correctivas.

- **Garantizar el liderazgo y compromiso del CIGD.**

Las actas de 2023 y 2024 muestran una ausencia de decisiones estratégicas y seguimiento sistemático al MSPI. Aunque en 2024 se socializó el autodiagnóstico, no hubo análisis comparativos, indicadores ni directrices claras. Esto refleja que el CIGD no ha asumido plenamente su rol de liderazgo y compromiso en la implementación del modelo.

Pese a las debilidades señaladas, se verificó que el CIGD cumple con algunos criterios del numeral 7.2.1:

- Adopción formal de la Política General de Seguridad y Privacidad de la Información y de los objetivos institucionales, según Acta No. 3 del 07/10/2024.
- Planeación y disposición de recursos financieros, humanos y tecnológicos para la implementación del MSPI, conforme a la lista de chequeo del numeral 7.4.1.
- Formalización de la conformación del CIGD y sus funciones en seguridad de la información mediante la Resolución 183 de 2018, que constituye el soporte normativo del Comité (aunque requiere actualización).

En síntesis, aunque se evidenció cumplimiento en la adopción de la política, la disposición de recursos y la formalización normativa del Comité, persisten debilidades significativas en la gobernanza, la comunicación, la evaluación de resultados, el seguimiento periódico y el compromiso estratégico del CIGD frente al MSPI.

OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025.

"Frente a lo expuesto (…) "En la verificación realizada sobre el numeral 7.2.1 del Documento Maestro del MSPI, se determinó que la entidad no cumple integralmente con las funciones de liderazgo y compromiso asignadas al CIGD, específicamente en lo relacionado con: garantizar la adopción de los requisitos del modelo en los procesos de la entidad, comunicar su importancia a nivel institucional, asegurar que el MSPI consiga los resultados previstos, realizar revisiones periódicas de su adopción con la participación del nominador, y garantizar el liderazgo y compromiso del Comité para alcanzar los objetivos de implementación"(…).

Me permito manifestar las siguientes precisiones:

Planes Institucionales

En cumplimiento del Decreto 612 de 2018, la entidad ha establecido el Plan de Gestión de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos, los cuales desarrollan las acciones

necesarias para dar respuesta a los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI.

El seguimiento a estos planes se realiza mensualmente, mediante el registro de avances y la consolidación de evidencias que dan cuenta de la ejecución de las actividades definidas. Este seguimiento permite identificar desviaciones, adoptar medidas de mejora y garantizar el cumplimiento progresivo de los objetivos establecidos.

Evidencias:

- *Plan de Gestión de Seguridad y Privacidad de la Información.*
- *Plan de Tratamiento de Riesgos.*
- *Carpeta de evidencias de seguimiento mensual a los planes.*

Seguimiento a la Implementación de la Política de Seguridad y Privacidad de la Información

De forma complementaria, se realiza un seguimiento trimestral al nivel de implementación de la Política de Seguridad y Privacidad de la Información, como eje estructural del SGSI. Esta actividad permite verificar el grado de cumplimiento de los lineamientos definidos y consolidar evidencias que soportan su apropiación institucional.

Evidencias:

- *Matriz de seguimiento a la implementación de la Política de Seguridad y Privacidad de la Información.*
- *Carpeta de evidencias del seguimiento trimestral.*

Estas actividades de seguimiento institucional, tanto a los planes como a la política, son coordinadas por el Equipo de Seguridad de la Información y dan cumplimiento al numeral 7.3 del documento INTI-M-001, así como al numeral 7.2.3 del MSPI, en cuanto al monitoreo y revisión periódica del Sistema de Gestión de Seguridad y Privacidad de la Información."

*En cumplimiento del numeral 7.1 literal h) del documento INTI-M-001 – Sistema de Gestión de Seguridad de la Información, la Alta Dirección de la Agencia Nacional de Tierras ha realizado la **designación formal y el respaldo institucional** de los roles estratégicos requeridos para la gestión de la seguridad de la información, a través de los siguientes mecanismos:*

- ***Resolución No. 202361002101356 del 4 de septiembre de 2023:** mediante este acto administrativo, la Alta Dirección designó formalmente a una servidora pública de planta para ejercer los roles de:*
  - *Oficial de Seguridad de la Información y Seguridad Digital.*
  - *Oficial de Protección de Datos Personales.*

*Este acto constituye el **mecanismo de delegación formal** y da cuenta del **compromiso de la Alta Dirección con el cumplimiento del Modelo de Seguridad y Privacidad de la Información – MSPI**, así como con lo dispuesto en el Decreto 620 de 2020 y la norma ISO/IEC 27001.*

- ***Resolución de nombramiento de Diana Lucía Herrera Riaño** como Subdirectora de Sistemas de Información de Tierras (SSIT), quien actualmente lidera la implementación del MSPI en la entidad.*

*Estas acciones evidencian el cumplimiento de la obligación de **designar y apoyar** los roles necesarios para una adecuada gestión de la seguridad de la información, en concordancia con los lineamientos del modelo.*

Conclusión SSIT

*Las evidencias entregadas en la etapa de solicitud de información dan cuenta de acciones concretas de liderazgo, seguimiento y compromiso institucional frente al MSPI. Por lo anterior, no resulta pertinente calificar la gestión como un **"incumplimiento integral"**, dado que la entidad ha adelantado mecanismos formales y sistemáticos que controvierten lo mencionado en la condición observada.*

*Con respeto al **Análisis,** me permito mencionar lo siguiente:*

Observación SSIT

Garantizar la adopción de los requisitos del MSPI en los procesos.

La observación indica que solo el 25% de los procesos han incorporado requisitos del MSPI. Sin embargo, este dato debe analizarse en el contexto de una implementación progresiva, conforme al ciclo PHVA. La ANT ha priorizado procesos misionales y críticos en la primera fase, lo cual es coherente con los principios de gestión de riesgos y focalización de recursos. La cobertura parcial no implica incumplimiento, sino una estrategia de escalamiento gradual

Comunicar en la entidad la importancia del MSPI.

Aunque se señala una cobertura del 17,53% en sensibilización, es importante destacar que la ANT ha desarrollado un plan de comunicación con enfoque multicanal, incluyendo capacitaciones, boletines, micrositios y espacios de formación. La medición de impacto está en proceso de fortalecimiento, pero la existencia del plan y su ejecución inicial demuestran compromiso institucional.

Asegurar que el MSPI consiga los resultados previstos.

El nivel de madurez del MSPI no debe evaluarse únicamente por la cobertura de procesos, sino por la efectividad de los controles implementados, la gestión de riesgos y la mejora continua. La ANT ha logrado avances en la formalización de políticas, asignación de recursos, y definición de roles, lo cual constituye una base sólida para alcanzar los resultados previstos. El autodiagnóstico es una herramienta de mejora, no una evidencia de incumplimiento.

Realizar revisiones periódicas de la adopción del MSPI.

La revisión del autodiagnóstico realizada en diciembre de 2024 constituye una acción de seguimiento válida. Aunque se recomienda efectuar dos revisiones anuales como buena práctica, la norma no establece esta exigencia de manera obligatoria. En el caso de la ANT, se realiza una revisión anual al

cierre de la vigencia, lo cual permite evaluar el avance en el nivel de madurez alcanzado durante el periodo.

Garantizar el liderazgo y compromiso del CIGD.

Se reitera lo mencionado del compromiso en el primer párrafo sobre esta observación

Conclusión SSIT:

La Agencia Nacional de Tierras ha demostrado acciones concretas y verificables en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), tales como la adopción de planes institucionales, la definición de roles estratégicos, la asignación de recursos y el seguimiento periódico de avances. Estas evidencias reflejan liderazgo, compromiso y cumplimiento progresivo de los requisitos establecidos.

Si bien se identifican oportunidades de mejora en la transversalización del modelo y en el fortalecimiento de las revisiones periódicas por parte del CIGD, ello corresponde a un proceso de madurez gradual y no a un incumplimiento integral. En este sentido, y conforme a lo dispuesto en la ***ISO/IEC 27001:2022 (numerales 5.1 Liderazgo y compromiso y 9.3 Revisión por la dirección),*** *la ANT cumple con los requisitos normativos, enmarcando las observaciones más como oportunidades de mejora que como no conformidades.*

Por lo anterior, respetuosamente solicitamos que la observación sea reconsiderada y reclasificada como ***Conformidad con oportunidad de mejora****, dado que se cumple el requisito, aunque se han identificado aspectos susceptibles de fortalecimiento."*

CONCLUSIÓN EQUIPO AUDITOR

En atención a la observación allegada por la SSIT frente a la No Conformidad Nro. 5 Debilidades en el liderazgo *y* compromiso del Comité Institucional de Gestión y Desempeño frente al MSPI, se precisa lo siguiente:

El hallazgo se fundamenta en el incumplimiento de lo dispuesto en el numeral 7.2.1 del Documento Maestro del MSPI, el cual establece como responsabilidades de la Alta Dirección y del CIGD: garantizar la adopción de los requisitos del modelo en los procesos institucionales, comunicar su importancia en la entidad, asegurar el logro de los resultados previstos, realizar revisiones periódicas de su adopción con la participación del nominador (mínimo dos veces por año), y demostrar liderazgo y compromiso para alcanzar los objetivos de implementación.

Si bien la SSIT expone que la entidad cuenta con planes institucionales, designación de roles estratégicos y seguimiento a políticas, estos elementos corresponden a acciones positivas de avance, pero no desvirtúan la condición observada, dado que:

- **Cobertura de procesos**: El autodiagnóstico 2024 evidenció que solo el 25% de los procesos institucionales incorporan requisitos del MSPI, lo cual no garantiza su adopción transversal en los términos exigidos por el numeral 7.2.1. La estrategia de implementación progresiva planteada no sustituye el cumplimiento integral del requisito.
- **Comunicación institucional**: La existencia de un plan de comunicación y algunas acciones ejecutadas no cumplen plenamente con la obligación de comunicar la importancia del modelo en toda la entidad, en tanto la cobertura es reducida (17,53% de funcionarios) y no se evidencian indicadores de impacto ni segmentación estratégica.
- **Revisiones periódicas**: El requisito es explícito en exigir al menos dos revisiones anuales con participación del nominador. La realización de una sola socialización en diciembre de 2024 no satisface este criterio, lo que confirma un incumplimiento normativo.
- **Resultados previstos**: El autodiagnóstico reflejó bajo nivel de madurez, cobertura limitada y avances reducidos en el ciclo PHVA, lo que demuestra que los resultados previstos no se han alcanzado en la medida requerida.
- **Liderazgo del CIGD**: Aunque existen resoluciones de designación de roles y evidencia de recursos asignados, las actas del CIGD no registran análisis estratégicos, comparativos ni decisiones que reflejen un acompañamiento directivo integral, lo que evidencia una gobernanza incompleta.

En este sentido, lo presentado por la SSIT constituye evidencia de acciones parciales o en curso, pero que no subsanan el incumplimiento frente al criterio de auditoría. La diferencia entre una Oportunidad de Mejora y una No Conformidad radica en que la primera señala aspectos a fortalecer sin contrariar un requisito obligatorio, mientras que la segunda corresponde a un incumplimiento directo de un requisito normativo o documental. En el presente caso, la ausencia de revisiones periódicas, la baja cobertura de procesos y la falta de evidencia de liderazgo estratégico del CIGD representan desviaciones frente a obligaciones establecidas en el Documento Maestro del MSPI, razón por la cual el hallazgo se mantiene como No Conformidad.

3.2.6. NO CONFORMIDAD Nro. 6. Debilidades en la documentación, aprobación, comunicación y alineación de la Política del MSPI con los objetivos institucionales.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI).** **Numeral 7.2.2.** Política de seguridad y privacidad de la información.

- Declaración de la Administración.
- Objetivos y Alcance.
- Cumplimiento Normativo.
- Compromiso con la Mejora Continua.
- Alineación con el Contexto de la Entidad.
- Asignación de Roles y Responsabilidades.
- Inclusión en el Comité de Gestión Institucional.
- Comunicación de la Política.

CONDICIÓN OBSERVADA:

En el marco de la auditoría realizada al Modelo de Seguridad y Privacidad de la Información (MSPI) y en cumplimiento de la normatividad vigente, en especial la Resolución 500 de 2021 del MinTIC y su Anexo 1 - Documento Maestro del MSPI, se observó que la Agencia Nacional de Tierras cuenta con una Política de Seguridad y Privacidad de la Información formalmente adoptada con código de calidad en el SIG INTI-Política-001 Política General de Seguridad y Privacidad de la Información v 5 del 29/10/2024.

ANÁLISIS:

La Agencia Nacional de Tierras cuenta con INTI-Política-001 Política General de Seguridad y Privacidad de la Información v 5 del 29/10/2024, la cual fue aprobada en Sesión 3 Comité Institucional de Gestión y Desempeño del 07/10/2024, estableciendo los principios, objetivos y compromisos institucionales para la gestión de la seguridad y privacidad de la información.

Se observó que la entidad difundió y socializó la política de Seguridad y Privacidad de la Información el 26 de febrero de 2025 entre sus servidores públicos y contratistas, promoviendo su apropiación y aplicación en los procesos institucionales, lo cual contribuye al fortalecimiento del sistema de gestión de la seguridad de la información.

Durante el desarrollo de la auditoría se pudo constatar que la política no tiene relacionado el marco normativo vigente como base para su constitución, se encuentra alineada parcialmente en especial con la Estrategia de Gobierno Digital y los lineamientos del MinTIC.

Asimismo, se observó que, dentro del documento se estableció el compromiso de cumplir con los requisitos relacionados con la seguridad y privacidad de la información y de mejorar continuamente el MSPI una vez adoptado.

El documento refleja el contexto de la ANT, aunque lo hace de manera implícita. Para mayor robustez y alineación con ISO 27001 / MSPI, es importante que el contexto esté descrito de forma explícita en un apartado que identifique claramente el contexto interno, externo, partes interesadas y alcance.

No se identifica la definición de roles y responsabilidades relacionados con la seguridad y privacidad de la información dentro del documento lo cual es un componente fundamental para la completitud de la Política.

No se identifica un Manual de Políticas de Seguridad de la Información que consolide políticas específicas aparte de la política general y el instructivo. Según buenas prácticas del SGS teniendo en cuanta el MSPI, se espera contar con un conjunto comprehensivo de políticas detalladas y específicas, claramente documentadas y disponibles para todos los colaboradores.
Si bien es cierto que se dispone de la política general y el instructivo, no se encontraron políticas específicas individuales en un manual unificado ni por separado.

Conforme con la verificación realizada, se da como no conformidad el contenido de la Política MSPI, como instrumento fundamental para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información institucional, debe incluir el marco normativo aplicable, el contexto de forma explícita y la definición de roles y responsabilidades en materia de seguridad de la información, asegurando alineación con ISO 27001 y el MSPI, el proceso de mejora continua, asegurando que la política sea actualizada, monitoreada y evaluada periódicamente y que esté de forma integral con los componentes requeridos.

No se identifica un Manual de Políticas de Seguridad de la Información que consolide políticas específicas aparte de la política general y el instructivo. Según buenas prácticas del SGS teniendo en cuanta el MSPI, se espera contar con un conjunto comprehensivo de políticas detalladas y específicas, claramente documentadas y disponibles para todos los colaboradores.

Si bien es cierto que se dispone de la política general y el instructivo, no se encontraron políticas específicas individuales en un manual unificado ni por separado.

OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025.

"Frente a lo mencionado (…) "No se identifica un Manual de Políticas de Seguridad de la Información que consolide políticas específicas aparte de la política general y el instructivo. Según buenas prácticas del SGS teniendo en cuanta el MSPI, se espera contar con un conjunto comprehensivo de políticas detalladas y específicas, claramente documentadas y disponibles para todos los colaboradores. Si bien es cierto que se dispone de la política general y el instructivo, no se encontraron políticas específicas individuales en un manual unificado ni por separado" (..)

Frente a lo observado, es importante precisar que la ANT sí cuenta con un documento que consolida las políticas específicas de seguridad de la información. Dicho documento corresponde al INTI-Política-008 – Lineamientos de Seguridad de la Información V4, el cual tiene como alcance "establecer lineamientos, reglas e instrucciones detalladas que permitan implementar un gobierno de seguridad de la información de la ANT, con el fin de proteger los activos de información y dar cumplimiento a los requisitos legales y a los estándares de seguridad de la Política de Gobierno Digital".

En este documento se encuentran desarrolladas de manera explícita las políticas específicas de seguridad de la información que complementan la Política General, tales como: Inventario de Activos de Información, Control de Acceso, Seguridad Física y Ambiental, Continuidad del Negocio, etc.

De esta manera, la ANT dispone de una estructura documental conformada por:

- *Política General de Seguridad y Privacidad de la Información (INTI-Política-001).*
- *Lineamientos de Seguridad de la Información (INTI-Política-008), que consolidan y desarrollan las políticas específicas.*
- *Procedimientos e instructivos asociados, que operacionalizan el cumplimiento de dichas políticas.*

Con lo anterior, se evidencia que la Entidad sí cuenta con un marco documental que incorpora tanto la política general como las políticas específicas requeridas por las buenas prácticas del SGSI y el MSPI.

2. Frente a lo mencionado: "El documento refleja el contexto de la ANT, aunque lo hace de manera implícita. Para mayor robustez y alineación con ISO 27001 / MSPI, es importante que el contexto esté descrito de forma explícita en un apartado que identifique claramente el contexto interno, externo, partes interesadas y alcance."
Es pertinente precisar que este aspecto ya fue abordado en la respuesta a la No Conformidad No. 1, en la cual se explicó y sustentó que el documento sí incorpora el contexto de la ANT, aunque de manera integrada dentro de sus apartados, y que por tanto no se comparte plenamente la observación realizada. En consecuencia, mantenemos la postura previamente expuesta, reiterando que la gestión del contexto (interno, externo, partes interesadas y alcance) está contemplada en el Sistema, conforme a lo sustentado en la NC No. 1.

3. Frente a lo mencionado: "No se identifica la definición de roles y responsabilidades relacionados con la seguridad y privacidad de la información dentro del documento lo cual es un componente fundamental para la completitud de la Política".
Es pertinente precisar que la definición de roles, responsabilidades y autoridades sí se encuentra identificada y formalizada en el documento INTI-M-001 Manual del Sistema de Gestión de Seguridad de la Información, específicamente en el numeral 7.3 Roles, responsabilidades y autoridades.
En este apartado se detallan los roles asignados a la Alta Dirección, el Comité Institucional de Gestión y Desempeño, el Oficial de Protección de Datos, el Oficial de Seguridad de la Información, el Equipo de Seguridad de la Información y la Oficina Asesora de Control Interno, estableciendo claramente sus responsabilidades y niveles de autoridad frente al MSPI.

En ese sentido, la entidad sí cumple con el requisito, dado que la definición solicitada se encuentra documentada y en aplicación, en coherencia con lo establecido en la Norma ISO/IEC 27001:2022 numeral 5.3 (Roles organizacionales, responsabilidades y autoridades).
Conclusión SSIT:

En atención a lo anterior, se concluye que la observación planteada no constituye una no conformidad, toda vez que la Agencia Nacional de Tierras sí dispone de los instrumentos documentales necesarios que consolidan políticas específicas de seguridad de la información, incorporan el análisis de contexto y definen roles, responsabilidades y autoridades de manera formal.
Estos elementos demuestran cumplimiento con los requisitos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) y en la Norma ISO/IEC 27001:2022, particularmente en lo dispuesto en los numerales 4.1, 4.2 y 5.3.

Por lo anterior, respetuosamente solicitamos que la observación sea reconsiderada y reclasificada como Conformidad de la implementación del MSPI, con oportunidad de mejora si así se estima pertinente, mas no como no conformidad."

CONCLUSIÓN EQUIPO AUDITOR

La Oficina de Control Interno observó la existencia de una Política General de Seguridad y Privacidad de la Información formalmente adoptada y difundida en la ANT; sin embargo, se evidenció que el documento no incorporó de manera explícita el marco normativo aplicable, la descripción formal del contexto institucional ni la definición de roles y responsabilidades dentro, además de no contar con un manual consolidado de políticas específicas alineadas al MSPI. La ausencia de estos elementos en la política limita la integralidad, trazabilidad y alineación de la política con los objetivos institucionales y debilita la gestión de seguridad de la información, genera riesgos en la asignación de responsabilidades y reduce la capacidad de garantizar valor público dando lugar al incumplimiento del numeral 7.2.2 del Documento Maestro del MSPI que establece la necesidad de contar con una política integral, clara y alineada a los objetivos institucionales y a los principios del SGSI. Donde las posibles causas pueden ser un enfoque parcial en la elaboración del documento de política, ausencia de

lineamientos metodológicos para consolidar políticas específicas en un manual único y la falta de revisión periódica para garantizar actualización y completitud del documento. Por lo anterior, y pese a las observaciones de la SSIT, se mantiene la No Conformidad Nro. 6.

Cabe precisar que un hallazgo de tipo No Conformidad se presenta cuando existe un incumplimiento verificable frente a un requisito normativo, lo cual exige la implementación de acciones de mejora. En contraste, una Oportunidad de Mejora corresponde a hallazgos de tipo conforme que no constituyen incumplimiento de los criterios normativos, pero que evidencian posibilidades de optimizar la eficiencia, eficacia o control en los procesos.

3.2.7. NO CONFORMIDAD Nro. 7. Debilidades en el esquema institucional de roles y responsabilidades para la implementación del MSPI.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI). Numeral 7.2.3.** Roles y responsabilidades.

- Aprobación y Comunicación de los roles y responsabilidades.
- Monitoreo del desempeño del MSPI.
- Reporte y seguimiento ante el Comité Institucional de Gestión y Desempeño.
- Delegar el equipo humano necesario para coordinar la implementación del MSPI
- La persona designada debe ser incluida como miembro del Comité de Gestión Institucional con voz y voto y en el Comité de Control Interno con voz.
- Asegurar que los funcionarios de la entidad conozcan qué se espera de ellos, cuál es su impacto en la seguridad de la información y de qué manera contribuyen con la adopción del MSPI.

CONDICIÓN OBSERVADA:

En el marco de la auditoría, se constató que si bien la entidad ha avanzado en la definición de roles y responsabilidades mediante el documento INTI-M-001 y en la designación de un Oficial de Seguridad de la Información, todavía existen aspectos que requieren fortalecimiento para dar cumplimiento integral al numeral 7.2.3. Entre ellos se encuentran:

- La aprobación formal y comunicación efectiva de los roles y responsabilidades establecidos.
- El monitoreo del desempeño del MSPI conforme a las funciones asignadas.

- El reporte y seguimiento oportuno ante el Comité Institucional de Gestión y Desempeño.
- La designación del equipo humano necesario para coordinar e implementar el modelo de forma operativa.
- La inclusión formal de la persona responsable como miembro del Comité de Gestión Institucional (con voz y voto) y del Comité de Control Interno (con voz).
- El aseguramiento de que los funcionarios conocen qué se espera de ellos, cuál es su impacto en la seguridad de la información y de qué manera contribuyen con la adopción del MSPI.

La condición observada podría estar asociada a debilidades en la gobernanza del MSPI dentro del CIGD, específicamente en el entendimiento de la importancia del modelo como parte de la agenda estratégica, lo que podría haber limitado la incorporación de acciones sistemáticas para su seguimiento y consolidación.

ANALISIS:

En la verificación realizada sobre el numeral 7.2.3 del Documento Maestro del MSPI, se analizaron distintos aspectos relacionados con la definición y cumplimiento de roles y responsabilidades institucionales. A continuación, se presenta el análisis de cada uno de estos elementos, destacando tanto los avances evidenciados como los aspectos que requieren fortalecimiento para garantizar la consolidación del MSPI en la entidad:

- **Aprobación y comunicación de roles y responsabilidades**. El INTI-M-001 describe de forma clara los actores y sus funciones, articulando áreas como SSIT, Jurídica, Talento Humano y Control Interno. Sin embargo, no se hallaron evidencias de una aprobación formal por parte de la Alta Dirección o el CIGD, ni de la comunicación oficial de todos los roles a la organización. Existen piezas gráficas elaboradas en 2025, pero su difusión está pendiente, lo que retrasa la apropiación institucional.

- **Monitoreo del desempeño del MSPI**. La entidad realiza seguimientos mensuales y trimestrales a planes específicos, lo cual es un avance importante. No obstante, no se encontró un informe consolidado, avalado por la Alta Dirección, que integre resultados, indicadores y análisis estratégico del MSPI como sistema. Esto restringe el valor de la información para la toma de decisiones.

- **Reporte al CIGD**. Se identificó que en 2023 no se presentaron informes formales sobre el MSPI. En 2024 se socializó el autodiagnóstico, lo que constituye un avance, pero aún con limitaciones frente a los criterios del modelo (ausencia de análisis comparativos, indicadores y recomendaciones estratégicas). El proceso requiere mayor estructuración y periodicidad.

➢ **Delegación del equipo humano**. El INTI-M-001 asigna funciones al Equipo de Seguridad, pero no se evidenció un acto administrativo que formalice su delegación. Se dispone de contratistas y enlaces, pero su integración no ha sido definida oficialmente.

➢ **Participación en comités institucionales**. El Subdirector de la SSIT, en calidad de Oficial de Seguridad, tiene participación formal en el CIGD con voz y voto, lo cual es un aspecto positivo. Sin embargo, no se constató su inclusión en el Comité de Control Interno (CICCI), lo que limita la articulación con los mecanismos de control interno.

➢ **Comprensión de roles por parte de funcionarios**. La encuesta aplicada en la UGT Pasto mostró fortalezas en el conocimiento de disposiciones de seguridad y en la respuesta a requerimientos, pero también debilidades en la asistencia a capacitaciones y en la cultura de reporte de incidentes. Esto sugiere la necesidad de reforzar los mecanismos de formación y comunicación institucional.

En conclusión, la entidad cuenta con avances importantes en la definición técnica de roles y responsabilidades, en la designación de un Oficial de Seguridad y en la articulación funcional de distintas dependencias. Sin embargo, aún persisten aspectos que requieren consolidación formal y estratégica, especialmente en materia de aprobación institucional, comunicación oficial, monitoreo integral, delegación documentada del equipo humano y fortalecimiento de la cultura organizacional en torno a la seguridad de la información.

OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025.

"Frente a lo expuesto, me permito manifestar que no comparto la calificación de No Conformidad, toda vez que:

1. ***Definición de Roles y Responsabilidades***
   - *El documento INTI-M-001 (Manual del SGSI, numeral 7.3) establece de manera clara los roles y responsabilidades institucionales en materia de seguridad de la información, en concordancia con lo exigido por el numeral 7.2.3 del Documento Maestro del MSPI.*
   - *Dicho manual articula dependencias como la SSIT, Jurídica, Talento Humano y Control Interno, incluyendo las funciones específicas del Oficial de Seguridad de la Información.*

2. ***Designación formal y participación en comités***
   - *Mediante acto administrativo, se ha designado a la subdirectora de la SSIT como Oficial de Seguridad de la Información, con participación formal en el CIGD con voz y voto, lo cual da cumplimiento directo al criterio del modelo.*
   - *Si bien no se constató aún la inclusión formal en el Comité de Control Interno (CICCI), esto corresponde a un aspecto de articulación administrativa que no implica incumplimiento del requisito principal, sino una oportunidad de fortalecimiento institucional.*

3. ***Monitoreo y reportes del MSPI***
   - *La entidad realiza seguimientos mensuales y trimestrales a los planes específicos del MSPI, y en 2024 presentó al CIGD el Autodiagnóstico MSPI, lo cual demuestra que existen mecanismos de seguimiento y reporte en funcionamiento.*
   - *La observación sobre la ausencia de un informe consolidado con indicadores estratégicos se reconoce como un aspecto susceptible de mejora, pero no como ausencia del cumplimiento requerido.*

4. ***Comunicación y apropiación institucional***
   - *Durante 2025, se elaboraron piezas gráficas y materiales de socialización de roles y responsabilidades, cuya difusión se encuentra en proceso.*

Conclusión SSIT

Con base en las evidencias descritas, se concluye que la Agencia Nacional de Tierras sí dispone de un marco institucional que da cumplimiento a lo exigido por el ***numeral 7.2.3 del Documento Maestro del MSPI*** *y por la* ***Norma ISO/IEC 27001:2022, numeral 5.3 (Roles organizacionales, responsabilidades y autoridades)****, al contar con roles y responsabilidades formalmente definidos, designados y documentados en el INTI-M-001, así como con mecanismos de seguimiento y reporte en ejecución.*
En este sentido, los hallazgos identificados corresponden a aspectos de fortalecimiento y mejora en la articulación, comunicación y consolidación de reportes, mas no a incumplimiento del requisito normativo.
Por lo anterior, respetuosamente se solicita la ***reclasificación del hallazgo como Observación u Oportunidad de Mejora****, en lugar de No Conformidad."*

CONCLUSIÓN EQUIPO AUDITOR

En atención a la observación allegada por la SSIT frente a la No Conformidad Nro. 7. Debilidades en el esquema institucional de roles y responsabilidades para la implementación del MSPI, se precisa lo siguiente:

- **Definición y aprobación formal de roles y responsabilidades**. El documento INTI-M-001 describe de manera clara los actores y sus funciones, aspecto valorado en la Conformidad Nro. 4. No obstante, de acuerdo con los numerales 7.2.3 "Roles y responsabilidades" y 9.1.3 "Revisión por la Dirección" del Documento Maestro del MSPI, todos los documentos que conforman el modelo deben contar con aprobación, para este caso es el Comité Institucional de Gestión y Desempeño (CIGD), en su calidad de máxima instancia de gobernanza del MSPI. Durante la auditoría no se evidenció dicha aprobación formal por parte del CIGD respecto de los roles y responsabilidades definidos en el INTI-M-001, lo que constituye un requisito aún pendiente.

- **Comunicación y socialización institucional**. El plan de comunicaciones institucional no contempla la socialización de roles y responsabilidades definidos en el INTI-M-001. La socialización iniciada por la SSIT en 2025 se realizó en el marco de la auditoría, sin estar planificada previamente como actividad sistemática, lo que limita su alcance y no garantiza la apropiación de los roles por parte de todos los funcionarios.
- **Monitoreo y reportes del MSPI**. Si bien existen seguimientos mensuales y trimestrales a planes específicos, no se constató la existencia de un informe consolidado del desempeño del MSPI como sistema, avalado por la Alta Dirección, que integre resultados, indicadores y análisis estratégicos. Este requisito es indispensable para cumplir integralmente lo dispuesto en el numeral 7.2.3 sobre monitoreo del desempeño del modelo.
- **Participación en comités institucionales.** Se verificó la participación del Oficial de Seguridad en el CIGD con voz y voto, en concordancia con el criterio. No obstante, no se acreditó su inclusión en el Comité de Control Interno (CICCI) con voz, tal como lo dispone expresamente el numeral 7.2.3, configurándose así un incumplimiento frente a un requisito obligatorio.

Las evidencias descritas en la observación de la SSIT confirman avances ya reconocidos en la Conformidad Nro. 4, particularmente en la definición técnica de roles y responsabilidades y en la designación del Oficial de Seguridad. Sin embargo, persisten incumplimientos frente a requisitos obligatorios del MSPI, relacionados con:

- La aprobación formal de los roles y responsabilidades por parte del CIGD, como instancia máxima de gobernanza.
- La planificación y ejecución de la socialización de roles, inexistente en el plan de comunicaciones institucional.
- La consolidación de informes de desempeño del MSPI avalados por la Alta Dirección.
- La inclusión formal del Oficial de Seguridad en el Comité de Control Interno (CICCI).

En consecuencia, el hallazgo se mantiene como No Conformidad, dado que se configuran incumplimientos verificables frente a los numerales 7.2.3 y 9.1.3 del Documento Maestro del MSPI.

3.2.8. NO CONFORMIDAD Nro. 8. Debilidades en el plan de comunicación, capacitación, sensibilización y concientización.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI) – MinTIC.**

Numeral 7.4.2. Competencia, toma de conciencia y comunicación.

La entidad debe definir un plan de comunicación, capacitación, sensibilización y concientización para:

- Asegurar que, las personas cuenten con los conocimientos, educación y formación o experiencia adecuada para la implementación y gestión del modelo.
- Involucrar al 100% de los funcionarios de la entidad en la implementación y gestión del MSPI.
- Concientizar a los funcionarios y partes interesadas en la importancia de la protección de la información.
- Identificar las necesidades de comunicaciones internas y externas relacionadas con la seguridad y privacidad de la información. Se deberá definir qué será comunicado, cuándo, a quién, quién debe comunicar y finalmente definir los procesos para lograrlo.

CONDICIÓN OBSERVADA:

Se evidenció que la entidad no cumple integralmente con lo establecido en el numeral 7.4.2 del Documento Maestro del MSPI, que exige la implementación de un plan estructurado de capacitación, sensibilización y comunicación. Dicho plan debe garantizar la formación adecuada del personal para la gestión del modelo, la participación del 100% de los funcionarios, la concientización tanto de los servidores como de las partes interesadas y la definición de las necesidades de comunicación internas y externas (qué se comunica, cuándo, a quién, por quién y mediante qué procesos). La ausencia de este cumplimiento expone a la entidad a una apropiación institucional limitada del MSPI, lo que podría afectar su eficacia y sostenibilidad en el tiempo.

Entre las causas identificadas para la condición observada se encuentra la inexistencia de rutas formativas diferenciadas según perfil, nivel de riesgo o rol institucional, así como una débil trazabilidad de los resultados de aprendizaje y de la percepción institucional. También se evidenció la falta de mecanismos formales para asegurar la cobertura total del personal, junto con la ausencia de acciones dirigidas a partes interesadas externas, como proveedores o aliados estratégicos.

ANÁLISIS:

Durante la verificación del numeral 7.4.2 del Documento Maestro del MSPI, se revisaron los documentos entregados por la Subdirección de Sistemas de Información de Tierras (SSIT) para la vigencia 2025, incluyendo el “Plan de cambio, cultura, apropiación, capacitación y sensibilización de Seguridad y Privacidad de la Información”, los reportes de asistencia, evaluaciones post-capacitación y el “Plan de Comunicaciones del MSPI”.

Si bien se identificaron acciones puntuales como capacitaciones generales, entrega de materiales gráficos e iniciativas de refuerzo vía correo electrónico, no se cumple de forma integral con el lineamiento ni con el propósito del numeral evaluado, por las siguientes razones:

- **Cobertura institucional insuficiente.** Con base en los listados de asistencia y consolidado de participación, se estima que solo el 17,53% de los funcionarios han sido capacitados, sin evidencia sin evidencia de control de duplicidades o validación de participación única. Esto incumple la exigencia de involucrar al 100% de los funcionarios.
- **Ausencia de formación diferenciada por rol.** No se ha desarrollado una estrategia pedagógica adaptada a los distintos perfiles institucionales. Las capacitaciones realizadas han sido de carácter general, sin adaptaciones según niveles de responsabilidad, criticidad de los activos o funciones dentro del MSPI, lo cual limita la efectividad del aprendizaje.
- **No inclusión de partes interesadas externas.** Se confirmó que, hasta la fecha, no se han realizado actividades de formación o sensibilización dirigidas a terceros como proveedores, contratistas externos o ciudadanía, desconociendo así el enfoque amplio de concientización exigido por el modelo.
- **Limitaciones en el plan de comunicaciones.** Aunque existe un documento titulado “Plan de Comunicaciones del MSPI”, este presenta debilidades en la definición de mensajes clave, cronograma detallado, indicadores de seguimiento y trazabilidad de resultados. No se evidencian mecanismos de evaluación del impacto comunicacional ni esquemas de retroalimentación continua.
- **Carencia de validación del nivel de apropiación.** No se cuenta con un informe consolidado que evalúe el nivel institucional de apropiación del modelo. Tampoco se han realizado encuestas de percepción ni acciones correctivas derivadas de los resultados de las evaluaciones post-capacitación, lo cual impide garantizar que los funcionarios comprendan su rol, responsabilidades y consecuencias del incumplimiento.

Resultados de la encuesta – UGT Pasto

En la encuesta aplicada a los funcionarios y contratistas de la UGT Pasto, se identificaron percepciones diferenciadas en torno a la asistencia a las capacitaciones del MSPI. Un grupo de participantes manifestó haber asistido a todas las jornadas programadas, mientras que otros indicaron haber participado únicamente en algunas actividades, al considerar que no todas eran relevantes para sus funciones. Adicionalmente, se registraron funcionarios que señalaron no haber asistido a ninguna capacitación, argumentando desconocimiento de las fechas o falta de información oportuna sobre los temas convocados.

Estos resultados evidencian que, además de la baja cobertura reflejada en los listados institucionales de asistencia, persisten limitaciones en la comunicación interna y en la difusión de las actividades formativas, lo que repercute en la apropiación institucional del modelo y en la efectividad de las acciones de capacitación.

En consecuencia, la entidad no cumple con lo establecido en el numeral 7.4.2 del Documento Maestro del MSPI, lo cual compromete la adecuada implementación del modelo, la madurez institucional en seguridad y privacidad de la información, y los principios de mejora continua y gestión del riesgo.

OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025.

"En atención a la no conformidad señalada, la entidad manifiesta lo siguiente:
La Subdirección de Sistemas de Información de Tierras (SSIT) cuenta con un ***Plan de cambio, cultura, apropiación, capacitación y sensibilización de Seguridad y Privacidad de la Información*** *debidamente formulado, en el cual se establecen actividades, cronograma, responsables y mecanismos de seguimiento, tal como se evidencia en el documento entregado en la etapa de solicitud de información de esta auditoría.*

Este plan contempla acciones de capacitación y sensibilización dirigidas a todo el personal de la entidad, garantizando así la ***cobertura al 100% en términos de acceso y convocatoria****. En este sentido, la entidad cumple con lo exigido por el numeral 7.4.2 del Documento Maestro del MSPI, en cuanto a la definición de un plan estructurado de comunicación, capacitación y concientización.*

Es importante precisar que, si bien la asistencia efectiva de los funcionarios a cada jornada depende de la disponibilidad y responsabilidades individuales, la obligación institucional se cumple al asegurar la ***difusión, accesibilidad y oferta formativa****. En consecuencia, la ausencia de algunos participantes no debe interpretarse como falta de cumplimiento por parte de la entidad, dado que la convocatoria se realizó de manera institucional y formal.*

Adicionalmente, se han implementado mecanismos de verificación mediante listados de asistencia, encuestas y evaluaciones post-capacitación, lo que permite medir la participación y percepción de los asistentes. La entidad reconoce que se pueden fortalecer aspectos como la diferenciación por perfiles, la inclusión de terceros externos y la consolidación de resultados de aprendizaje; sin embargo, estas oportunidades de mejora no implican la inexistencia del plan ni la ausencia de acciones.

Conclusión SSIT

Por lo anterior, se considera que el hallazgo descrito no constituye una No Conformidad, en la medida en que se da cumplimiento formal al criterio evaluado, conforme a lo establecido en el ***numeral 7.4.2 del Documento Maestro del MSPI*** *y en la* ***ISO/IEC 27001:2022, numeral 7.3 (Conciencia)****, que exige*

asegurar que el personal sea consciente de sus responsabilidades en materia de seguridad de la información mediante procesos de capacitación y comunicación.
En consecuencia, se solicita respetuosamente que la observación sea reevaluada y reclasificada como ***Oportunidad de Mejora o Recomendación****, más no como No Conformidad, considerando que la entidad cuenta con un plan estructurado, mecanismos de seguimiento y acciones de sensibilización en ejecución."*

CONCLUSIÓN EQUIPO AUDITOR

En atención a las observaciones allegadas por la SSIT respecto a la No Conformidad Nro. 8, se precisa lo siguiente:

El numeral 7.4.2 del Documento Maestro del MSPI establece que la entidad debe definir y ejecutar un plan de comunicación, capacitación, sensibilización y concientización que asegure:

- La formación adecuada de las personas en relación con sus roles.
- El involucramiento del 100% de los funcionarios en la gestión del modelo.
- La concientización tanto de funcionarios como de partes interesadas externas.
- La definición clara de qué se comunica, cuándo, a quién, quién comunica y cómo se evalúan los resultados.

Durante la verificación se evidenció que:

- **Cobertura institucional insuficiente.** La participación alcanzó solo el 17,53% del personal, sin mecanismos que aseguren la cobertura total exigida. La convocatoria institucional, aunque formal, no reemplaza la obligación de garantizar el involucramiento del 100% de los funcionarios.
- **Ausencia de formación diferenciada por rol.** Las capacitaciones han sido generales y no existe una estrategia pedagógica adaptada a distintos perfiles o responsabilidades, lo cual limita la efectividad del aprendizaje.
- **No inclusión de partes interesadas externas.** No se encontraron actividades dirigidas a contratistas, proveedores u otros actores, incumpliendo el alcance amplio de concientización que dispone el modelo.
- **Limitaciones del plan de comunicaciones.** El documento no define mensajes clave, cronograma detallado, indicadores ni mecanismos de evaluación del impacto. Tampoco contemplaba la socialización de roles y responsabilidades, iniciada únicamente en el marco de la auditoría.

Estos aspectos evidencian un incumplimiento directo del numeral 7.4.2, por lo que no se limitan únicamente a oportunidades de fortalecimiento. En este sentido, una No Conformidad corresponde a la contravención verificable de un requisito obligatorio del MSPI, con impacto en el cumplimiento del modelo. En contraste, una Oportunidad de Mejora aplica cuando el requisito se cumple, pero se identifican elementos susceptibles de optimización.

Dado que lo observado compromete el cumplimiento del requisito mismo (cobertura total, inclusión de externos, formación diferenciada y plan estructurado), se mantiene la calificación de No Conformidad.

3.2.9. NO CONFORMIDAD Nro. 9. Debilidades en la planificación e implementación de controles.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI). Numeral 8.1** Planificación e implementación.

CONDICION OBSERVADA:

La Agencia Nacional de Tierras cuenta con los documentos Mapa de Riesgos de Seguridad de la Información - versión 2 – 2025 publicado el 3 de febrero de 2025 y Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025 publicado el 29 enero de 2025.

A continuación, se presenta un análisis para en relación con el cumplimiento del numeral 8.1 "Planificación e implementación" del Modelo de Seguridad y Privacidad de la Información (MSPI), enfocado en la verificación del Plan de implementación de controles de seguridad y privacidad de la información y la evidencia de su ejecución.

ANALISIS:

De acuerdo con la revisión realizada por la Oficina de Control Interno respecto al cumplimiento del numeral 8.1 Planificación e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), y teniendo en cuenta el cumplimiento del numeral 7.3.2 "Valoración de los riesgos de seguridad de la información" como entrada base, se observó que la Agencia Nacional de Tierras (ANT) cuenta con:

- **Plan de Implementación.**

Se evidenció que la Agencia Nacional de Tierras cuenta con un documento denominado "Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información**"**, el cual contiene:

- **Controles y actividades específicas.** Acciones como elaboración de planes de trabajo, actualización de instructivos y socialización de matrices.
- **Fechas de inicio y fin.** Las acciones preventivas tienen cronogramas definidos, sin embargo, los controles no.
- **Responsables asignados.** Cada acción preventiva cuenta con un responsable claro, sin embargo, no hay claridad del responsable para cada control.
- **Metas.** Se incluyen productos esperados, unidad de medida y metas cuantificables.
- **Seguimiento.** Se puede identificar si las actividades han sido "Reportadas" o "No reportadas", y si se ha realizado cargue de evidencia.

- **Efectividad.**

La Oficina de Control Interno realiza la revisión de la matriz matriz-riesgos-seguridad-de-la-informacion-ant-2024 donde observó:

- El mapa permite identificar los riesgos relevantes con los responsables.
- Algunos riesgos tienen controles formulados, pero no en todos los casos se evidencia periodicidad clara ni una trazabilidad que asegure continuidad.
- La documentación de causas y consecuencias está bien identificada, pero no siempre se enlaza a acciones preventivas específicas.
- La valoración del riesgo (probabilidad/impacto) se realiza, pero los controles no siempre se alinean a reducir dicho nivel residual de manera verificable.
- Se evidencian deficiencias en la formulación de los controles del mapa de riesgos de seguridad de la información, en aspectos de frecuencia, documentación y soporte de evidencias, la efectividad está limitada.

En la matriz (Hoja Dirección General), los riesgos cuentan con causas y consecuencias documentadas, sin embargo:

- Algunos controles no tienen periodicidad definida o suficiente.
- No siempre se vinculan acciones preventivas específicas a los riesgos de mayor impacto.
- Se dificulta la trazabilidad y verificación de la gestión de riesgos.
- Aumenta la probabilidad de materialización de incidentes de seguridad.

- Se reduce la eficacia del Sistema de Gestión de Seguridad de la Información y del cumplimiento del MSPI.

Al analizar el Mapa de Riesgos de Seguridad de la Información, se evidenció que, aunque la Agencia Nacional de Tierras ha identificado riesgos relevantes junto con sus causas, consecuencias y una valoración inicial de probabilidad e impacto, la efectividad de los controles definidos resulta limitada. Esto obedece a que no todos los riesgos cuentan con acciones preventivas claramente formuladas, la frecuencia de ejecución de los controles es baja en algunos casos y no se dispone de evidencias documentales suficientes que permitan verificar su cumplimiento y trazabilidad. En consecuencia, el mapa cumple solo de manera parcial con su propósito de gestionar los riesgos de seguridad de la información, requiriendo fortalecimiento en la definición de acciones de control, la periodicidad de su aplicación y la consolidación de evidencias que respalden su implementación y efectividad. Por lo anterior, la Oficina de Control Interno concluye como No Conformidad, dado que, si bien la entidad ha desarrollado la planificación del MSPI conforme al numeral 8.1 “Planificación e Implementación”, persisten oportunidades de mejora que deben atenderse para garantizar un control integral y efectivo de los riesgos de seguridad de la información.

OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025.

“En relación con la no conformidad observada, es importante precisar que la entidad sí cuenta con instrumentos documentales y metodológicos que soportan la adecuada planificación, implementación y seguimiento de los controles de seguridad de la información, conforme al numeral 8.1 del Documento Maestro del MSPI.

En particular, se encuentran definidos y en aplicación los siguientes documentos los cuales fueron aportados en la etapa de Solicitud de Información:

1. Plan de Cierre de Brechas MSPI:

o Documento que consolida los controles enmarcados en el ciclo PHVA, incluyendo la identificación de brechas, actividades de cierre, responsables y cronogramas.

o Este plan asegura que los controles no solo estén identificados, sino que también cuenten con responsables asignados y actividades calendarizadas para su ejecución.

2. Procedimiento para la Administración de Riesgos de Seguridad de la Información - DEST–P-011:

o Establece la metodología institucional para la identificación, valoración, tratamiento y seguimiento de los riesgos asociados a la seguridad de la información.

o Define claramente las responsabilidades, periodicidad de revisión y mecanismos de trazabilidad.

3. Mapa de Riesgos y Plan de Tratamiento de Riesgos de Seguridad de la Información:

o Permiten articular los riesgos identificados con los controles implementados, evidenciando su gestión dentro del marco de mejora continua y gestión preventiva.

4. Seguimiento a la Implementación de la Política de Seguridad y Privacidad de la Información

o De forma complementaria, se realiza un seguimiento trimestral al nivel de implementación de la Política de Seguridad y Privacidad de la Información, como eje estructural del SGSI. Esta actividad permite verificar el grado de cumplimiento de los lineamientos definidos y consolidar evidencias que soportan su apropiación institucional, a través de Matriz de seguimiento a la implementación de la Política de Seguridad y Privacidad de la Información.

Conclusión SSIT

En este sentido, se considera que se cumple con la exigencia de planificar y establecer mecanismos de control, toda vez que cuenta con instrumentos normativos y operativos que estructuran la gestión de riesgos y la implementación de controles de seguridad de la información.

Por lo anterior, solicitamos que la No Conformidad No. 9 sea reevaluada, teniendo en cuenta la evidencia documental existente y la integración de los planes y procedimientos mencionados, en concordancia con lo establecido en el numeral 8.1 del Documento Maestro del MSPI y el numeral 8.1 de la ISO/IEC 27001:2022 (Planificación y control operacional), que disponen la necesidad de asegurar que los procesos se planifiquen, implementen, controlen y mantengan de manera efectiva para el cumplimiento de los requisitos de seguridad de la información"

CONCLUSIÓN EQUIPO AUDITOR

Teniendo en cuenta las observaciones de la SSIT, la Oficina de Control Interno observó que, aunque la Agencia Nacional de Tierras cuenta con documentos como el Plan de Cierre de Brechas, el Procedimiento de Administración de Riesgos, el Mapa y el Plan de Tratamiento de Riesgo.

Se observó, vacíos en la definición de periodicidad, asignación de responsables y acciones preventivas específicas, lo que limita la trazabilidad y dificulta comprobar la efectividad de la gestión, incumpliendo lo dispuesto en el numeral 8.1 del Documento Maestro del MSPI y en la norma ISO/IEC 27001:2022, que requieren asegurar la adecuada planificación, implementación, seguimiento y eficacia de los controles de seguridad de la información

El desarrollo parcial del proceso de gestión de riesgos y controles afecta la eficacia del MSPI, reduce la capacidad de la entidad para anticipar y prevenir incidentes de seguridad, limita la trazabilidad de las acciones y pone en riesgo la coherencia y confiabilidad del SGSI. Esta situación puede tener origen en la ausencia de lineamientos claros para definir la periodicidad y responsables del seguimiento, la falta de acciones preventivas específicas en los planes establecidos, la débil articulación entre los documentos de riesgos y la implementación de controles, así como en la debilidad en la aplicación de

los procedimientos. Por lo anterior, se mantiene la No Conformidad Nro. 9, dado que el proceso se encuentra desarrollado solo de forma parcial, con riesgos que afectan la eficacia del MSPI

Cabe precisar que un hallazgo de tipo No Conformidad se presenta cuando existe un incumplimiento verificable frente a un requisito normativo, lo cual exige la implementación de acciones de mejora. En contraste, una Oportunidad de Mejora corresponde a hallazgos de tipo conforme que no constituyen incumplimiento de los criterios normativos, pero que evidencian posibilidades de optimizar la eficiencia, eficacia o control en los procesos.

3.2.10. NO CONFORMIDAD Nro. 10. Debilidades en el seguimiento, medición, análisis y evaluación del MSPI.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI) – MinTIC.**

Numeral 9.1.1. Seguimiento, medición, análisis y evaluación.

CONDICIÓN OBSERVADA:

Se evidenciaron debilidades en el seguimiento, medición, análisis y evaluación del MSPI, contraviniendo lo dispuesto en el numeral 9.1.1 del Documento Maestro, que establece la obligación de contar con hojas de vida de indicadores e incluirlos en el tablero de control del Plan de Acción (Decreto 612 de 2018), presentar reportes periódicos y documentados sobre el desempeño del modelo, definir tiempos y recursos previstos para el monitoreo con evidencia de aceptación y retroalimentación por parte del CIGD, y desarrollar la evaluación de efectividad con base en los controles definidos en el Plan de Tratamiento de Riesgos.

Lo observado limita la capacidad institucional para evaluar la eficacia del modelo, identificar brechas y orientar la toma de decisiones estratégicas en materia de seguridad y privacidad de la información.

La situación observada podría estar asociada a limitaciones en la definición y documentación de los indicadores, a la ausencia de procedimientos estandarizados para la elaboración y presentación periódica de informes consolidados, y a la falta de asignación específica de tiempos y recursos para el monitoreo. Asimismo, podría estar vinculada a una articulación insuficiente del MSPI con los espacios de validación y retroalimentación del CIGD y a la integración parcial de la evaluación con los controles definidos en el Plan de Tratamiento de Riesgos, lo que en conjunto restringe la capacidad de seguimiento sistemático del modelo.

ANÁLISIS:

En la verificación realizada sobre el numeral 9.1.1 del Documento Maestro del MSPI, se revisaron los instrumentos metodológicos definidos por la entidad, así como la evidencia documental presentada para demostrar su aplicación práctica. El análisis incluyó la revisión de las hojas de vida de indicadores y su incorporación en el tablero de control, los reportes periódicos de desempeño presentados al CIGD, los informes de evaluación de efectividad de controles, y la articulación entre la metodología formal y la trazabilidad de las decisiones estratégicas. A continuación, se presentan los principales hallazgos identificados en cada uno de estos aspectos:

- **Hoja de vida de indicadores e inclusión en tablero del Plan de Acción.**

El manual INTI-M-001 y el procedimiento DEST-P-007 establecen que los indicadores deben documentarse utilizando el formato DEST-F-002 y gestionarse a través del tablero de control corporativo. En la verificación realizada, se observó que las fichas remitidas por la SSIT el 04/08/2025 no corresponden al formato DEST-F-002 y no incorporan todos los campos mínimos requeridos para la medición y el análisis, conforme a lo dispuesto en el DEST-P-007 y a las recomendaciones de la Guía MinTIC de Indicadores de Gestión de Seguridad de la Información.

De igual manera, al revisar los cuatro planes institucionales (Plan de Acción 2025, PETI, Plan de Tratamiento de Riesgos y Plan de Seguridad y Privacidad de la Información), no se identificó evidencia de inclusión de dichos indicadores como parte del tablero de control ni de su articulación explícita en los instrumentos de planificación.

- **Reporte periódico y documentado del desempeño del MSPI al CIGD.**

De la revisión de las actas de 2023 y 2024 se constató que durante 2023 no se registraron reportes relacionados con el desempeño del MSPI. En la vigencia 2024, en la 4ª sesión del Comité (19 de diciembre), se incluyó la socialización del autodiagnóstico de seguridad y privacidad de la información por parte de la Subdirección de Sistemas de Información de Tierras (SSIT). Este espacio representó un avance en términos de visibilidad del modelo en la agenda del Comité; sin embargo, el registro documental da cuenta de que la presentación se limitó a exponer los resultados generales del autodiagnóstico, sin incluir análisis comparativos respecto a años anteriores, indicadores de desempeño, metas de cierre de brechas o recomendaciones estratégicas. Asimismo, el acta no refleja que se hubieran generado decisiones ni retroalimentación del Comité en relación con la socialización.

En este sentido, desde el nivel estratégico, el seguimiento, medición, análisis y evaluación del MSPI no se evidencia de manera integral, pues no se cuenta con un proceso sistemático, periódico y consolidado de reporte ante el CIGD que permita garantizar la trazabilidad del control ni la retroalimentación institucional previstos en el numeral 9.1.1

- **Informe de evaluación de la efectividad de controles del Plan de Tratamiento de Riesgos.**

La Agencia sí genera un informe de medición de controles de seguridad de la información, en coherencia con lo dispuesto en el Plan de Tratamiento de Riesgos. No obstante, el contenido de dicho informe se centra en el cumplimiento operativo de actividades y no desarrolla plenamente una evaluación de efectividad con base en indicadores analíticos ni presenta retroalimentación formal del CIGD. En consecuencia, el lineamiento del numeral 9.1.1 se cumple de manera parcial, al existir la evidencia documental del informe, pero sin consolidar el análisis estratégico ni el uso institucional de los resultados para decisiones de mejora.

- **Seguimiento, medición, análisis y evaluación con indicadores y decisiones.**

La metodología corporativa (DEST-P-007 + DEST-F-002) está definida; sin embargo, la evidencia operativa (fichas SSIT no estandarizadas y ausencia de tablero institucional) no permite demostrar un ciclo completo de medición-análisis-decisión con indicadores críticos, tendencias y acciones correctivas formalizadas/seguimiento por el CIGD. Por tanto, el requerimiento del 9.1.1 se cumple parcialmente en el diseño metodológico, pero no en su aplicación y trazabilidad institucional.

- **Propósito de evaluar el desempeño de la Seguridad de la Información y eficacia del MSPI.**

El propósito de evaluar el desempeño de seguridad de la información y la eficacia del MSPI no se cumple integralmente. Si bien existen instrumentos formales (manuales, políticas, planes, fichas de indicadores, informes de implementación), su aplicación práctica presenta limitaciones:

- Los indicadores no están estandarizados ni incluidos en el tablero de control.
- El CIGD no recibe reportes sistemáticos ni adopta decisiones basadas en el desempeño del modelo.
- Los informes de controles existen, pero carecen de un enfoque analítico que permita valorar la eficacia en la mitigación de riesgos.

En consecuencia, la trazabilidad del seguimiento y la utilidad para la toma de decisiones estratégicas aún es reducida, lo que impide afirmar que el numeral 9.1.1 cumple su propósito.

OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025.

*"El **numeral 9.1.1 del MSPI (ISO 27001)** pide que la organización defina **qué medir, cómo, con qué métodos y con qué frecuencia**, para evaluar la eficacia del SGSI.*

*En el contexto del sector público en Colombia, ese requerimiento se **articula directamente** con:*

- ***Decreto 612 de 2018** → Obliga a las entidades a integrar los planes institucionales en un **Plan de Acción anual**, donde el **Plan de Tratamiento de Riesgos** hace parte integral.*
- *El **Plan de Tratamiento de Riesgos de Seguridad de la Información** ya está formulado, contiene actividades específicas de mitigación y **tiene seguimiento mensual**.*
- *El seguimiento se evidencia en reportes de ejecución y en los informes de avance que alimentan el **Plan de Acción institucional**.*

*Entonces, lo que la auditoría llama "tablero" realmente ya existe, solo que **con otro nombre y en el marco de la norma local**:*

- *El tablero que pide ISO 27001 / MSPI puede entenderse como el **mecanismo de seguimiento y consolidación** de los indicadores.*
- *En la ANT ese rol lo cumple el **Plan de Tratamiento de Riesgos → Plan de Acción (Decreto 612) → Seguimiento mensual**, que ya está institucionalizado.*

*Se concluye sí **hay un tablero**, pero se denomina "Plan de Acción" y es el instrumento oficial exigido por el Decreto 612.*

A continuación se explica la relación anteriormente expuesta:

Numeral / Requisito	***Qué exige***	***Normativa Nacional Relacionada***	***Evidencia en la ANT***	***Interpretación***
MSPI / ISO 27001 – 9.1.1 Seguimiento, medición, análisis y evaluación	*La organización debe determinar: qué necesita medir, métodos de seguimiento, medición, análisis, evaluación,*	***Decreto 612 de 2018** → Obliga a integrar los planes institucionales en un **Plan de Acción**, incluyendo los de seguridad de la*	*- **Plan de Tratamiento de Riesgos de Seguridad de la Información** (incluye controles, actividades, responsables*	*El "tablero" solicitado por la auditoría ya existe, solo que se materializa en el **Plan de Acción institucional** con seguimiento*

Numeral / Requisito	***Qué exige***	***Normativa Nacional Relacionada***	***Evidencia en la ANT***	***Interpretación***
	cuándo se mide, quién lo hace, y cómo asegurar la validez de los resultados. Además, se debe conservar evidencia como información documentada .	*información, con seguimiento y evaluación periódica.*	*, cronograma). - **Plan de Acción Institucional** que incorpora el plan de riesgos, en cumplimiento del Decreto 612. - **Seguimiento mensual** documentado a las actividades y riesgos. - **Indicadores SGSI** registrados en matriz (archivo Excel).*	*mensual, más los **indicadores del SGSI**. Es decir, se cumple el requisito, aunque con una denominación diferente.*

<u>Conclusión SSIT</u>

*La observación levantada no constituye una **No Conformidad**, en la medida en que la entidad sí cumple con lo exigido en el numeral 9.1.1 del Documento Maestro del MSPI y en la ISO/IEC 27001. Si bien no se utiliza el término "tablero de control", el requisito se encuentra implementado a través de:*

- ***El Plan de Tratamiento de Riesgos de Seguridad de la Información**, que contiene controles, actividades, responsables y cronograma.*
- ***El Plan de Acción Institucional**, en cumplimiento del Decreto 612 de 2018, donde se integra el seguimiento y evaluación periódica de dichos riesgos.*
- ***Los Indicadores del SGSI**, que permiten medir, analizar y evaluar la eficacia de la gestión de seguridad y privacidad de la información.*
- ***El seguimiento mensual** documentado, que asegura trazabilidad, validez de resultados y mejora continua.*

*En este sentido, el mecanismo de control existe, está documentado y es funcional, aunque con una denominación distinta a la utilizada por "tablero". Por lo tanto, la entidad sí **cumple el requisito** y lo*

*evidenciado corresponde más a una **diferencia de interpretación terminológica** que a un incumplimiento real del MSPI.*
Por lo anterior, se considera que esta situación no constituye una No Conformidad."

CONCLUSIÓN EQUIPO AUDITOR

En atención a la observación presentada por la SSIT, se precisa que el numeral 9.1.1 del Documento Maestro del MSPI establece que los indicadores deben documentarse en fichas estandarizadas e integrarse en el tablero de control del Plan de Acción, con el fin de garantizar trazabilidad, análisis sistemático y retroalimentación de la Alta Dirección. En la verificación realizada se constató que:

- Las fichas de indicadores entregadas no corresponden al formato metodológico establecido ni incluyen todos los campos requeridos para su análisis y trazabilidad.
- No se evidenció la vinculación de los indicadores en los cuatro planes institucionales (Plan de Acción 2025, PETI, Plan de Tratamiento de Riesgos y Plan de Seguridad y Privacidad de la Información), lo que limita su visibilidad en la planeación estratégica y en el seguimiento integral del modelo.
- Las actas del CIGD no registran retroalimentación ni decisiones sustentadas en los indicadores, lo que impide completar el ciclo de seguimiento–análisis–decisión prevista en el numeral 9.1.1.
- El informe de evaluación de la efectividad de controles del Plan de Tratamiento de Riesgos existe, pero se limita a un enfoque operativo de ejecución de actividades, sin un análisis integral de eficacia con base en indicadores ni validación formal del CIGD.

Lo anterior evidencia debilidades en el cumplimiento del numeral 9.1.1 que comprometen la trazabilidad y el uso estratégico del seguimiento del MSPI, configurando una No Conformidad.

Es importante precisar que una No Conformidad corresponde a la contravención verificable de un requisito obligatorio del MSPI, afectando el cumplimiento del modelo. Por el contrario, una Oportunidad de Mejora aplica cuando el requisito sí se cumple, pero se identifican aspectos que podrían optimizarse. En este caso, el incumplimiento radica en que los indicadores definidos en la política no forman parte de los instrumentos formales de planeación y seguimiento, razón por la cual el hallazgo se ratifica como No Conformidad.

3.2.11. NO CONFORMIDAD Nro. 11. Debilidades en la revisión por la dirección del MSPI.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI). Numeral 9.1.3.** Revisión por la Dirección.

CONDICIÓN OBSERVADA:

Se evidenció que la Agencia Nacional de Tierras no ha desarrollado integralmente el proceso de revisión por la dirección establecido en el numeral 9.1.3 del Documento Maestro del MSPI. Si bien la Política de Seguridad y Privacidad de la Información fue aprobada en el Comité Institucional de Gestión y Desempeño (CIGD), no se encontró evidencia de aprobación formal del Manual INTI-M-001, pese a que este documento establece que todos los instrumentos del MSPI deben contar con aprobación formal.
De la revisión de las actas del CIGD correspondientes a 2023 y 2024, se identificó que en 2023 no se recibieron reportes relacionados con el desempeño del MSPI y que en 2024 se presentó el autodiagnóstico de seguridad y privacidad de la información. Sin embargo, dicho informe se limitó a una socialización general y no incluyó análisis comparativos con años anteriores, metas de cierre de brechas, indicadores de desempeño ni registro de decisiones estratégicas derivadas de su discusión.

Lo anterior contraviene lo dispuesto en el Documento Maestro del MSPI, que establece la obligación de que la Alta Dirección revise periódicamente el modelo para garantizar su conveniencia, adecuación y eficacia. Esta situación limita la capacidad institucional para asegurar la trazabilidad, el control y la mejora continua en la gestión de la seguridad y privacidad de la información.

La ausencia de revisión integral del MSPI podría deberse a la falta de lineamientos internos que aseguren la aprobación formal de todos los documentos del modelo, más allá de la Política de Seguridad. Tampoco se identificó un cronograma definido para revisiones periódicas en el CIGD, lo que ha derivado en un seguimiento limitado a socializaciones puntuales, como el autodiagnóstico 2024. Asimismo, los reportes elaborados no se han consolidado en informes estratégicos con indicadores, análisis comparativos y recomendaciones para la Alta Dirección, lo que refleja un enfoque más operativo que estratégico. Finalmente, el proceso de seguimiento ha sido gestionado de forma reactiva y no mediante un esquema planificado y continuo de revisión por la dirección.

ANÁLISIS:

En la verificación realizada sobre el numeral 9.1.3 del Documento Maestro del MSPI, se evaluó el proceso de revisión por la dirección, considerando la aprobación de documentos del modelo, las actas del CIGD de 2023 y 2024, los reportes presentados, así como la trazabilidad de decisiones y retroalimentación por parte de la Alta Dirección. El análisis incluyó tanto los aspectos formales de aprobación y documentación, como la práctica de socialización y seguimiento de los resultados del MSPI en instancias estratégicas. A continuación, se presentan los hallazgos identificados en cada uno de estos elementos:

- **Aprobación de documentos del MSPI.** El Manual INTI-M-001 establece que todos los documentos del MSPI deben ser aprobados, incluidos los actos administrativos necesarios para formalizarlos. En las actas revisadas del CIGD (2023 y 2024) consta la aprobación de la Política de Seguridad y Privacidad de la Información, pero no se evidenció aprobación del Manual INTI-M-001 ni de otros documentos técnicos claves (planes de tratamiento de riesgos, plan de seguridad). Esta ausencia limita la trazabilidad formal de la revisión por parte de la Alta Dirección.
- **Revisión en el CIGD (2023).** En las sesiones 1, 2 y 3 de 2023 no se registraron presentaciones, informes ni discusiones sobre el MSPI. Los temas tratados correspondieron a otros asuntos institucionales, sin abordar seguimiento ni desempeño del modelo.
- **Revisión en el CIGD (2024).** En la sesión N.º 4 de diciembre de 2024 se incluyó la socialización del autodiagnóstico de seguridad y privacidad de la información, liderada por la Subdirección de Sistemas de Información de Tierras. La evidencia muestra que fue una exposición general, sin comparación frente a resultados previos, sin indicadores de desempeño, sin metas de cierre de brechas ni propuestas de acciones de mejora. Tampoco se registraron observaciones o decisiones estratégicas del Comité derivadas de esta presentación.
- **Propósito del numeral.** El Documento Maestro establece que la revisión por la dirección debe permitir conocer avances, logros y metas, y garantizar la aceptación de los resultados por parte del CIGD. Las actas revisadas no evidencian este proceso de manera integral, ya que no se documenta un seguimiento sistemático ni la retroalimentación de la Alta Dirección.
- **Impacto.** La ausencia de revisión integral, periódica y documentada limita la capacidad institucional para evaluar la eficacia del MSPI, identificar brechas y orientar decisiones de alto nivel en seguridad y privacidad de la información.

La revisión por la dirección del MSPI no se cumple integralmente, ya que no se evidencia la aprobación de todos los documentos requeridos, ni la existencia de un proceso sistemático y periódico de revisión del desempeño, resultados y metas del modelo por parte del CIGD. La ausencia de decisiones y retroalimentación documentada limita la capacidad de la entidad para asegurar la eficacia y sostenibilidad del MSPI, en contravención a lo establecido en el numeral 9.1.3 del Documento Maestro.

OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025.

"Se considera respetuosamente que este hallazgo no constituye una No Conformidad, dado que la revisión por la dirección del MSPI sí se ha ejecutado en el marco institucional previsto, con las siguientes evidencias:

1. ***Instancia formal de revisión:***

La revisión por la dirección se efectúa en el Comité Institucional de Gestión y Desempeño (CIGD), el cual hace parte de los miembros con voz y voto la Alta Dirección, de conformidad con la normativa interna del Comité como el órgano de aprobación y seguimiento de políticas y lineamientos institucionales.

2. ***Documentos aprobados:***
   - *En actas del CIGD de 2023 consta la aprobación de la Política de Seguridad y Privacidad de la Información.*
   - *El Plan de Tratamiento de Riesgos y el Plan de Seguridad de la Información, exigido por el Decreto 612 de 2018 y que forma parte integral del Plan de Acción Institucional, se encuentra aprobado y en ejecución, con seguimiento mensual documentado.*
   - *Se cuenta adicionalmente con el Plan de Cierre de Brechas del MSPI y el Procedimiento para la Administración de Riesgos de Seguridad de la Información, que soportan la planeación, seguimiento y control del modelo, entre otros documentos que hacen parte integral del sistema.*
3. ***Seguimiento y análisis realizados:***
   - *En la sesión N.º 4 de diciembre de 2024 del CIGD, se presentó el Autodiagnóstico de Seguridad y Privacidad de la Información, lo cual evidencia que los resultados del MSPI han sido informados y revisados por la Alta Dirección.*
   - *Aunque el informe tuvo un carácter general, cumplió el propósito del numeral 9.1.3 de garantizar que la dirección conociera los avances y resultados del modelo.*
4. ***Cumplimiento del requisito:***

*El numeral 9.1.3 establece la obligación de que la Alta Dirección revise periódicamente el modelo para asegurar su **conveniencia, adecuación y eficacia**. Lo anterior ya se cumple en la ANT, puesto que:*
   - *Existe una instancia definida de revisión (CIGD).*
   - *Se han aprobado formalmente instrumentos clave (Política de Seguridad, Plan de Tratamiento de Riesgos, Plan de Seguridad de la Información).*
   - *Se han realizado ejercicios de socialización, análisis y seguimiento que permiten a la Alta Dirección tomar conocimiento del desempeño del MSPI.*

Conclusión SSIT:

*De conformidad con lo expuesto, se evidencia que la Agencia Nacional de Tierras (ANT) da cumplimiento a la **Revisión por la Dirección** del Modelo de Seguridad y Privacidad de la Información (MSPI), en concordancia con lo establecido en el **numeral 9.3 de la Norma ISO/IEC 27001:2022 (Revisión por la Dirección)** y con el **numeral 9.1.3 del Documento Maestro del Sistema**.*

El 8 de mayo de 2025, la SSIT solicitó formalmente a la Oficina de Planeación la creación de un espacio estratégico para la presentación de hallazgos, seguimiento, compromisos e indicadores del Sistema de Gestión de Seguridad de la Información (SGSI), denominado Comité de Seguridad de la Información de la Entidad, con participación de los líderes de proceso. En respuesta, el 15 de mayo de 2025, la Oficina de Planeación indicó que el ***Comité Institucional de Gestión y Desempeño*** *constituye el espacio idóneo para abordar la estrategia institucional en materia de seguridad y ciberseguridad, de conformidad con lo dispuesto en la* ***Resolución 183 de 2018*** *y en virtud de su composición directiva.*
En este sentido, el aspecto señalado en el informe corresponde a una ***oportunidad de mejora orientada a fortalecer la trazabilidad de la información reportada a la Alta Dirección****, y no a una No Conformidad, toda vez que la entidad cumple con lo establecido en la* ***ISO/IEC 27001:2022, numeral 9.3 (Revisión por la Dirección)****.*

Por lo anterior, se solicita respetuosamente a la Oficina de Control Interno la ***reevaluación de la No Conformidad N.º 11****, considerando la evidencia documental aportada y el cumplimiento normativo expuesto."*

CONCLUSIÓN EQUIPO AUDITOR

En atención a la observación allegada por la SSIT frente a la No Conformidad Nro. 11. Debilidades en la revisión por la dirección del MSPI, se precisa lo siguiente:

- Si bien el Comité Institucional de Gestión y Desempeño (CIGD) aprobó la Política de Seguridad y Privacidad de la Información, no existe evidencia de aprobación formal del Manual INTI-M-001 ni de otros documentos técnicos del modelo, lo que limita la trazabilidad formal y el cumplimiento del requisito de gobernanza establecido en el numeral citado.
- En 2023 no se registraron revisiones ni reportes del MSPI en las actas del CIGD, incumpliendo la exigencia de revisión periódica por la dirección.
- En 2024 se socializó el autodiagnóstico de seguridad y privacidad, pero su alcance fue limitado: no incluyó indicadores de desempeño, análisis comparativos con vigencias anteriores, metas de cierre de brechas ni registro de decisiones estratégicas del Comité. Por tanto, no se cumple con el propósito del numeral 9.1.3 de garantizar la conveniencia, adecuación y eficacia del MSPI.

En este sentido, las evidencias aportadas por la SSIT demuestran avances operativos (planes formulados, socializaciones, seguimiento al plan de riesgos), pero no desvirtúan la condición observada, dado que el requisito central de aprobación integral de documentos y revisión sistemática por la Alta Dirección no se encuentra cumplido.

En este caso, lo evidenciado constituye una No Conformidad, al verificarse la contravención de un requisito obligatorio del numeral 9.1.3 del Documento Maestro del MSPI. A diferencia de una Oportunidad de Mejora, que aplica cuando el requisito se cumple, pero existen aspectos susceptibles de optimización, lo observado refleja la ausencia de un cumplimiento integral del criterio. En consecuencia, se ratifica la No Conformidad Nro. 11, dado que persisten debilidades en la revisión por la dirección que comprometen la trazabilidad, eficacia y sostenibilidad del modelo.

3.2.12. NO CONFORMIDAD Nro. 12. Debilidades en el Plan Anual de Mejora del MSPI.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI). Numeral. 10.1.** Mejora.

  - Actividades concretas de mejora.
  - Responsables definidos.
  - Cronograma y seguimiento.
  - Evidencias de ejecución.
  - Aprobación por el Comité respectivo.

- **Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG**, versión 6 de diciembre del 2024.

CONDICION OBSERVADA:

La Agencia Nacional de Tierras (ANT) adoptó el Modelo de Seguridad y Privacidad de la Información (MSPI) mediante un Sistema de Gestión de Seguridad de la Información (SGSI), con políticas y planes codificados que incluyen diagnóstico, seguimiento, evaluación y mejora. Así mismo, cuenta con un Plan de Cierre de Brechas del MSPI, que identifica brechas, recomendaciones, actividades de mejora, responsables y porcentaje de avance. La Entidad también elabora el Plan de Tratamiento de Riesgos y lo actualiza en cada ciclo o cuando sea necesario.

ANÁLISIS:

El numeral 10.1 "Mejora" del MSPI establece la obligación de implementar un proceso de mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información, y este debe articularse con las tres líneas de defensa organizacionales para garantizar un control integral y efectivo.

- **Articulación con las tres líneas de defensa.**

Línea de Defensa	Responsabilidad en la Mejora Continua (10.1 MSPI)
1ª Línea: Dueños de procesos	➢ Implementar los controles de seguridad y privacidad definidos. ➢ Aplicar las acciones de mejora en sus procesos. ➢ Identificar nuevos riesgos o brechas en la operación diaria.
2ª Línea: Áreas de control, riesgo y seguridad de la información	➢ Conformada por servidores que ocupan cargos del nivel directivo o asesor (media o alta gerencia), quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección. ➢ Liderar la elaboración y actualización del Plan Anual de Mejora. ➢ Acompañar y asesorar a la primera línea en la implementación de acciones. ➢ Definir indicadores de seguimiento. ➢ Garantizar la alineación con el Plan Estratégico de Seguridad de la Información. ➢ Asegurar que, los controles y la gestión del riesgo de la primera línea sean adecuados y efectivos, mediante actividades de seguimiento, verificación y autoevaluación, orientando a la gestión institucional y generando alertas oportunas a la Alta Dirección.
3ª Línea: Auditoría interna / Control Interno	➢ Realizar auditorías internas para verificar la ejecución y efectividad del Plan Anual de Mejora. ➢ Emitir hallazgos, recomendaciones y verificar el cierre de acciones correctivas. ➢ Validar el cumplimiento del ciclo PHVA (Planificar, Hacer, Verificar, Actuar) en la gestión del MSPI.

Tabla 3. 3*Articulación con las Tres Líneas de Defensa (Numeral 10.1 MSPI.)*
Fuente: *Creación propia*

La mejora continua bajo el numeral 10.1 debe ser un proceso estructurado, medible, auditado y con roles diferenciados según las líneas de defensa, garantizando sostenibilidad, madurez en la gestión de la seguridad y cumplimiento normativo.

- **Responsabilidad de la Segunda Línea de Defensa.**

La Segunda Línea de Defensa tiene como responsabilidad principal diseñar, estructurar y liderar la formulación del Plan Anual de Mejora del MSPI, asegurando su articulación con el Plan Estratégico de Seguridad de la Información. Asimismo, debe definir los indicadores de gestión, cumplimiento y eficacia del plan, coordinar el seguimiento periódico al avance de las actividades de mejora y generar los reportes correspondientes para la alta dirección. Igualmente, le corresponde asesorar y acompañar a la primera línea de defensa en la implementación efectiva de las acciones de mejora, así como proponer la actualización del plan cuando se identifiquen nuevos riesgos o brechas.

Sin embargo, mediante comunicación oficial del 14 de julio de 2025, la Subdirección de Sistemas de Información y Tecnología (SSIT) informó que actualmente la entidad no cuenta con un Plan Anual de Mejora aprobado y ejecutado, conforme lo exige el numeral 10.1 del MSPI, argumentando que la presente auditoría corresponde a la primera evaluación formal del modelo en la entidad.

Adicionalmente, se observó la ausencia de un Plan Anual de Mejora aprobado, reflejando una debilidad en la gestión atribuible a la Segunda Línea de Defens**a**, en la medida en que no se lideró la elaboración estructurada de dicho plan conforme a lo exigido en el numeral 10.1 del MSPI. Se evidenció una falta de acompañamiento estructurado a la primera línea de defensa, lo que ha limitado la implementación de acciones correctivas y de mejora continua.

Se evidenció un retroceso en el nivel de cumplimiento de controles específicos, (Tabla 3 Controles con retroceso) en comparación con la medición anterior, disminuyendo el porcentaje alcanzado en el plan de cierre de brechas. Esto refleja la ausencia de acciones sostenibles que garanticen la mejora continua y la madurez del sistema.

Fuente	Id. Item	Cargo	Item	Descripción	Brecha 2023	Nivel de Cumplimiento 2023	Nivel de Cumplimiento 2024
Administrativas	AD.5.1.3	Responsable de la Continuidad	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.		Realizar pruebas de funcionalidad de los procesos, procedimientos y controles de la continuidad de la seguridad de la información.	20	0
Administrativas	AD.6.2.2	Control interno	Cumplimiento con las políticas y normas de	Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad	revisar periódicamente el cumplimiento de las normas de seguridad	60	0

			seguridad.	organizacional.	de la información para los sistemas de información.		
Administrativas	AD.6.2.3	Responsable de SI	Revisión de cumplimiento técnico.	Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.	Realizar las evaluaciones pertinentes	20	0
Técnicas	T.7.1.5	Responsable de SI	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Documentar el impacto de los incidentes	60	0
Técnicas	T.7.1.6	Responsable de TICs	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad	Documentar las directrices a la guía de gestión de incidentes	20	0

				o el impacto de incidentes futuros.			

Tabla 4. 4*Controles con retroceso*
Fuente: *Creación Propia*

Con base en la respuesta remitida por la Subdirección de Sistemas de Información de Tierras (SSIT) a través de correo electrónico el 16/07/2025 respecto al avance del Plan de Cierre de Brechas, se evidencia que la Agencia Nacional de Tierras (ANT) ha adelantado acciones para mitigar los retrocesos detectados en el cumplimiento de controles críticos de seguridad y privacidad de la información. Se tienen aspectos positivos como:

- La ANT formuló un Plan de Cierre de Brechas – Vigencia 2024, que incluye acciones específicas para atender los controles con nivel de cumplimiento en cero.
- Existen avances parciales en la actualización de procedimientos críticos, como: Plan de Continuidad de Negocio (BCP) y Plan de Recuperación ante Desastres (DRP), Procedimiento de Gestión de Incidentes con guías complementarias se encuentra en elaboración, Implementación del Centro de Operaciones de Seguridad (SOC).
- Hay acciones programadas con fechas estimadas de cierre para el 2do semestre de 2025, pero no todas tienen fecha.

No obstante, se observó que, si bien es cierto que tienen un plan de brechas:

- Este no cumple las características de un Plan Anual de Mejora, el cual debe estar formalmente aprobado y articulado al Plan Estratégico de Seguridad de la Información, integral y estratégico como lo exige el MSPI.
- Ausencia de un cronograma integral y oficializado que consolide todas las actividades de mejora continua, sus responsables, recursos, plazos con control de avances y productos entregables.
- Falta definición de indicadores de desempeño y eficacia para medir el impacto real de las acciones implementadas sobre la madurez del MSPI.
- Las acciones de mejora en curso no se encuentran aún validadas, formalizadas ni aprobadas por un Comité Institucional competente, lo que limita la trazabilidad y gobernabilidad del proceso.
- Se mantienen retrocesos en niveles de cumplimiento en controles clave frente a la medición 2023, lo que demuestra debilidad en la sostenibilidad de los controles implementados.

Donde la falta de definición e implementación formal de un Plan Anual de Mejora específico para el MSPI y la débil articulación entre el Plan de Cierre de Brechas y los requisitos establecidos en el numeral 10.1 del MSPI, pueden ocasionar:

- Riesgo de estancamiento o retroceso en la madurez de la gestión de la seguridad y privacidad de la información en la entidad.
- Limitaciones para garantizar la sostenibilidad de los controles implementados y la mejora continua requerida por el MSPI.
- Pérdida de trazabilidad en la ejecución y control de las acciones de mejora.

La Oficina de Control Interno identifica la necesidad de que la Agencia Nacional de Tierras (ANT) diseñe, formalice, apruebe e implemente un Plan Anual de Mejora del MSPI, en cumplimiento del numeral 10.1 del Modelo de Seguridad y Privacidad de la Información (MSPI) donde se debe:

- **Definir, aprobar e implementar un Plan Anual de Mejora del MSPI.** Con actividades concretas de mejora, Cronograma detallado de ejecución con plazos por actividad, responsables designados por cada acción, Revisión periódica para actualizarlo frente a riesgos emergentes, Registro y publicación del plan y sus avances en la Intranet o página institucional para promover la transparencia, Asignar un responsable anual explícito incluyendo un suplente y Alinearlo con el PETI.

- **Reflejar indicadores de desempeño y eficacia.** Para medir el impacto de las acciones tales como: % de riesgos evaluados con plan de tratamiento activo, % de acciones implementadas según cronograma, Publicar trimestralmente en un dashboard el estado de los indicadores, Incluir un Indicador Primario: “% de cumplimiento del Documento Maestro MSPI anual”, % de reducción de brechas, N° de riesgos críticos mitigados y Nivel de madurez alcanzado en MSPI.

La Oficina de Control Interno define como No Conformidad el incumplimiento frente al numeral 10.1 “Mejora" del MSPI y la responsabilidad como Segunda Línea de Defensa indicada en el MIPG:

> (…) “Aquí *se incluyen a los jefes de planeación, o quienes hagan sus veces; coordinadores de equipos de trabajo, coordinadores de sistemas de gestión, gerentes de riesgos (donde existan), líderes o coordinadores de contratación, financiera y de TIC, entre otros que se deberán definir acorde con la complejidad y misionalidad de cada organización. Esto le permite a la entidad hacer un seguimiento o autoevaluación permanente de la gestión, de manera que pueda orientar y generar alertas a las personas que hacen parte de la 1ª línea de defensa, así como a la Alta Dirección (Línea Estratégica).*

Esta línea se asegura de que los controles y procesos de gestión del riesgo de la 1ª línea de defensa sean apropiados y funcionen correctamente, además, se encarga de supervisar la eficacia e implementación de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas que permitan adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos." (…)

En razón a que la Agencia Nacional de Tierras (ANT) no cuenta con un Plan Anual de Mejora del MSPI alineado con el Plan Estratégico de Seguridad de la Información, que se encuentre aprobado, formalizado, implementado y con mecanismos de seguimiento establecidos.

El avance reportado por la SSIT evidencia una gestión que no configura el cumplimiento pleno del numeral 10.1 "Mejora" del MSPI, el cual exige:

- Un Plan Anual de Mejora formal y aprobado.
- Alineación con el Plan Estratégico de Seguridad de la Información.
- Integración del ciclo de mejora continua (PHVA) como práctica institucionalizada.

La situación representa una oportunidad de mejora que debe ser abordada de manera prioritaria. La ausencia del plan limita la capacidad institucional para garantizar el proceso de mejora continua en la gestión de la seguridad y privacidad de la información, afectando la sostenibilidad de los controles implementados, el fortalecimiento de la madurez en el modelo y el cumplimiento de las obligaciones establecidas en el Documento Maestro del MSPI.

OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025.

"La observación de la No Conformidad planteada en relación con el numeral 10.1 "Mejora" del Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI), no es procedente por las siguientes razones:

1. Primera auditoría formal:

Esta auditoría corresponde a la primera evaluación formal del Sistema de Gestión de Seguridad de la Información (SGSI) implementado en la Agencia Nacional de Tierras (ANT). Por lo tanto, el ciclo de mejora continua apenas inicia y los insumos necesarios para estructurar un Plan Anual de Mejora formalizado se derivan precisamente de esta primera auditoría.

2. Existencia de un Plan de Cierre de Brechas:

La ANT cuenta con un Plan de Cierre de Brechas del MSPI, resultado de la evaluación inicial del modelo, en el que se identifican brechas, recomendaciones, actividades de mejora, responsables y nivel de avance. Dicho plan constituye una acción de mejora continua en los términos del numeral 10.1 del MSPI, ya que permite optimizar procesos y atender riesgos identificados.

3. Cumplimiento del lineamiento de mejora continua:

El numeral 10.1 del Documento Maestro del MSPI establece que las entidades deben elaborar un plan de mejoramiento continúo basado en las siguientes entradas:

- *Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI*
- *Resultados de auditorías*
- *Revisiones independientes al MSPI.*

En este caso, el plan de brechas elaborado cumple con ese propósito, en tanto:

- *Recoge los hallazgos de la evaluación inicial.*
- *Define responsables y actividades de mejora.*
- *Registra avances parciales en controles críticos (ej. BCP, DRP, gestión de incidentes, SOC).*
- *Integra acciones programadas con fechas estimadas de cierre para el segundo semestre de 2025.*

4. Norma no taxativa:

Si bien la buena práctica recomendada es contar con un Plan Anual de Mejora con cronograma e indicadores, la norma no establece la obligatoriedad rígida de su emisión en la primera auditoría. Por el contrario, señala que el plan debe construirse a partir de los resultados de auditorías y revisiones. Dado que esta es la primera auditoría, es razonable que los insumos para el plan integral se formalicen a partir de esta revisión.

5. Ciclo de madurez en construcción:

La mejora continua en el marco del MSPI y del MIPG debe ser entendida como un proceso gradual y progresivo. En esta etapa, el avance en la ANT está orientado a la consolidación del modelo, a la identificación de brechas y al fortalecimiento de controles. De ahí que el Plan de Cierre de Brechas vigente constituya el instrumento inicial de mejora, que será la base para la formulación del Plan Anual de Mejora en la siguiente vigencia.

Conclusión SSIT

En coherencia con lo dispuesto en la ISO/IEC 27001:2022, numerales 9.3 (Revisión por la dirección), 10.1 (No conformidad y acción correctiva) y 10.2 (Mejora continua), se concluye que:

- *La mejora continua debe basarse en los resultados de auditorías y revisiones, y dado que esta corresponde a la primera auditoría formal del SGSI en la ANT, los insumos para la construcción del Plan Anual de Mejora apenas se consolidan.*
- *La existencia de un Plan de Cierre de Brechas vigente constituye una acción de mejora continua válida, en línea con los numerales citados.*
- *Por lo anterior, la No Conformidad No. 12 no da lugar y sea reevaluada, teniendo en cuenta lo expuesto y sustentado anteriormente mencionado." (…).*

CONCLUSIÓN EQUIPO AUDITOR

Después de analizar las observaciones allegadas por la SSIT, la Oficina de Control Interno concluyó que, si bien la Agencia Nacional de Tierras dispone de un Plan de Cierre de Brechas y ha adelantado acciones parciales de mejora, este instrumento no cumple con las características exigidas para un Plan

Anual de Mejora del MSPI. Se observó la ausencia de un plan formal, aprobado y articulado con el Plan Estratégico de Seguridad de la Información, así como la falta de un cronograma consolidado, indicadores de desempeño y validación por parte del Comité competente.

Se incumple lo establecido en el numeral 10.1 del Documento Maestro del MSPI y en los lineamientos del MIPG, los cuales exigen que la organización cuente con un Plan Anual de Mejora formal, aprobado y articulado con los objetivos estratégicos del sistema. Estas debilidades limitan la trazabilidad y sostenibilidad de los controles, afectan la capacidad de la entidad para garantizar la mejora continua del SGSI y generan riesgos en cuanto a la madurez, eficacia y continuidad del MSPI.

La situación puede estar asociada a la falta de lineamientos metodológicos claros para la elaboración del plan, la ausencia de mecanismos de articulación con el Plan Estratégico de Seguridad de la Información, debilidades en la definición de indicadores y cronogramas de seguimiento, así como a la limitada gestión del Comité competente en la validación y aprobación del documento.

Conforme con lo anterior, la Oficina de Control Interno mantiene la No Conformidad Nro. 12, dado que la gestión de mejora se encuentra desarrollada solo de manera parcial y no asegura la madurez, eficacia ni continuidad requeridas por el MSPI.

Cabe precisar que un hallazgo de tipo No Conformidad se presenta cuando existe un incumplimiento verificable frente a un requisito normativo, lo cual exige la implementación de acciones de mejora. En contraste, una Oportunidad de Mejora corresponde a hallazgos de tipo conforme que no constituyen incumplimiento de los criterios normativos, pero que evidencian posibilidades de optimizar la eficiencia, eficacia o control en los procesos.

3.2.13. NO CONFORMIDAD Nro. 13. Debilidades en la implementación de Procedimientos de Seguridad de la Información UGT Pasto.

CRITERIO:

- **Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI). Numeral 8.1.** Planificación e Implementación

- **ADMBS-P-014** Administración de cuentas de usuario y acceso a recursos tecnológicos, versión 6 del 20/09/2023.

CONDICION OBSERVADA:

Conforme con la verificación realizada por la Oficina de Control Interno se observó que el procedimiento:

- Está alineado con normas y marcos de referencia como la ISO 27001 y el MSPI, lo que garantiza que contemple principios de seguridad de la información.
- Define con claridad la trazabilidad del proceso (solicitud → validación → creación/ajuste/inactivación → asignación de privilegios → respuesta), lo cual debería evitar que un usuario opere con credenciales prestadas.
- Exige documentación formal (formas ADMBS-F072, F073, F078, acuerdo de confidencialidad) como requisito previo para la creación o novedad de usuarios, lo que asegura la legalidad y autenticidad del acceso.
- Establece controles específicos como: Validación de autorización de solicitudes, Creación de usuarios únicos con datos completos y asociados a su cargo, Inactivación automática de cuentas al finalizar contratos, Política de cambio de contraseña en el primer ingreso, Limita el uso de cuentas genéricas a casos excepcionales y con responsable identificado, evitando accesos no atribuibles.

ANÁLISIS:

Se realizó prueba en la UGT Pasto, con encuesta desde el 13 al 19 de agosto a los funcionarios y contratistas sobre: En el desarrollo de sus funciones, ¿Alguna vez ha tenido que utilizar el usuario y contraseña de otro funcionario o contratista para acceder a las aplicaciones de la Agencia? Obteniendo los siguientes datos:

Respuesta	Cantidad	%
No, siempre he utilizado un usuario asignado a mi nombre.	45	52%
Sí, actualmente lo hago.	3	3%
Sí, pero fue en el pasado y ya tengo usuario propio.	15	17%
No respondieron la encuesta	0	0%
Total	**87**	**100%**

Tabla 5. *5Cuentas de Usuario*
Fuente*. Encuesta UGT Pasto*

La Oficina de control Interno identificó que:

- El 52% (45 funcionarios/contratistas) indicó que siempre utiliza su propio usuario y contraseña, lo cual refleja un nivel positivo de cumplimiento de los lineamientos del MSPI sobre la autenticación individual y la responsabilidad personal en el uso de credenciales.
- Un 3% (3 personas) manifestó que actualmente utiliza credenciales de terceros, lo que representa un riesgo alto para la seguridad de la información, ya que vulnera los principios de confidencialidad, trazabilidad y control de accesos.

- El 17% (15 personas) afirmó que en el pasado hizo uso de credenciales de otros, pero que actualmente cuentan con un usuario propio. Esto evidencia una mejora frente a la gestión de accesos, aunque también refleja que en algún momento existieron deficiencias en los procesos de asignación oportuna de usuarios.
- El 28% restante (24 personas) no se refleja en los primeros tres grupos, lo que sugiere que hubo posibles limitaciones para el diligenciamiento de la encuesta.

No obstante, a pesar de la existencia del procedimiento, el 20% de los encuestados manifestó haber usado credenciales de terceros en algún momento (17% en el pasado y 3% en la actualidad). Esto evidencia una brecha entre lo establecido y la práctica real.

El hecho de que aún haya usuarios compartiendo cuentas indica que:

- No siempre se asignan credenciales de manera oportuna al inicio de funciones.
- Existe falta de control en la verificación de cumplimiento de este procedimiento por parte de la Mesa de Servicios y responsables de TI.
- Hay debilidad en la cultura de seguridad y en la concienciación de funcionarios y contratistas sobre los riesgos y responsabilidades del uso indebido de credenciales.

El procedimiento contempla controles (como inactivaciones automáticas y validación de solicitudes), pero no se observa un mecanismo robusto de monitoreo continuo que detecte y alerte el uso indebido de cuentas como accesos simultáneos con un mismo usuario.

El procedimiento ADMBS-P-014 es técnicamente sólido, bien documentado y alineado con buenas prácticas de seguridad; sin embargo, los resultados de la consulta en la UGT Pasto muestran que su implementación y cumplimiento presentan debilidades prácticas.

El hecho de que un porcentaje de colaboradores reconozca el uso de credenciales de terceros revela que:

- No se están aplicando en su totalidad los controles definidos en el procedimiento.
- Persiste un riesgo alto de pérdida de trazabilidad, confidencialidad y responsabilidad sobre las acciones realizadas en los sistemas.
- La entidad requiere reforzar tanto la ejecución técnica del procedimiento como asignación inmediata de usuarios, bloqueo de cuentas compartidas y cultura organizacional con sensibilización permanente.

La OCI tuvo en cuenta que existen 79 contratistas vinculados a la UGT Pasto, base de datos aportada por la UGT Pasto “UGT NARIÑO Persoanl.xlsx” para lo cual se realizó la selección de una muestra (36) y se obtuvo:

Licencia	Cantidad	%
Office 365 E1	21	**58%**
Office 365 E3	2	**6%**
Office 365 E1 Plus	7	**19%**
Sin Licencia	6	**17%**
Total	**36**	**100%**

Tabla 6. 6*Licencias*
Fuente*: BD_EIST*

Se observó que el 17% de los contratistas no cuentan con licencia para el uso de su cuenta de correo institucional, donde 2 de ellos se encuentra vinculados desde el mes de mayo de 2025, 1 desde el 19/09/2024 y 1 para los meses de junio, julio y agosto. Lo que puede conllevar al uso no adecuado de las cuentas de usuario y la posible vulnerabilidad de la integridad de la Información.

Los resultados muestran que, aunque más de la mitad de los encuestados cumple adecuadamente con el uso de credenciales personales, persisten prácticas inadecuadas de intercambio de usuarios y contraseñas (20% entre uso actual y pasado) que comprometen la seguridad de la información en la Agencia.

El procedimiento ADMBS-P-014 es técnicamente sólido, bien documentado y alineado con buenas prácticas de seguridad; sin embargo, los resultados de la consulta en la UGT Pasto y la aplicación de la muestra en colaboración con el EIST, teniendo en cuenta la falta de Licencias incumplen su implementación.

OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025.

"Se reconoce la No Conformidad señalada, toda vez que no se ha reportado la materialización de un riesgo en el marco del procedimiento establecido. Es importante precisar que, de acuerdo con el alcance definido, la responsabilidad primaria de dicho procedimiento corresponde a la Secretaría General y no a la SSIT.
No obstante, desde la SSIT se han realizado acciones de control y seguimiento mediante monitoreos periódicos sobre los usuarios, contribuyendo de esta manera a la detección y gestión temprana de posibles incidentes.
En coherencia con lo anterior, se acepta la No Conformidad, comprometiéndose la entidad a articular las acciones con la Secretaría General a fin de fortalecer la trazabilidad y asegurar el cumplimiento integral del procedimiento."

CONCLUSION EQUIPO AUDITOR

Teniendo en cuenta las observaciones de la SSIT y en análisis por parte del equipo auditor de la Oficina de Control Interno se concluye que se mantiene la No Conformidad Nro.13.

4. EVALUACIÓN PLAN DE MEJORAMIENTO

El equipo auditor verificó las acciones de mejora asociadas al alcance de la auditoría, observando que:
( ) no hay acciones de mejora a la espera de determinar su efectividad.
(**X**) se evaluó la efectividad de las siguientes acciones de mejora:

En cuanto a la evaluación del plan de mejoramiento, se verificó la efectividad de las acciones implementadas frente a los hallazgos identificados en auditorías anteriores, con el propósito de determinar si estas lograron subsanar las causas que les dieron origen y si contribuyen al fortalecimiento del MSPI.

Actividad Origen	Informe Seguimiento Gestión de Riesgos de Gestión e Informáticos		
No. Hallazgo	C2	**Código Acción (es)**	AMI-259, AMI-260, AMI-261, AMI-262, AMI-263
Causa Raíz	Desactualización de la política de seguridad de la información y mapa de riesgos de seguridad de la información		
Acción de mejora	➢ Realizar la actualización de la política de seguridad de la información ➢ Realizar seguimiento a la implementación de la política de seguridad de la información ➢ Realizar la publicación en el SIG del procedimiento de administración de riesgos de seguridad de la información ➢ Formulación del mapa de riesgos de seguridad de la información fortaleciendo las acciones de control y preventivas ➢ Implementar una herramienta o sistema de información que permita gestionar de manera eficiente los riesgos de seguridad de la información, brindando seguimiento, alertas tempranas, modificaciones y administración para las acciones de control y preventivas, así como su materialización para cada uno de los riesgos establecidos		
Estado Efectividad	Efectiva ( ) Inefectiva (**X**)		
Auditor Verificador	Diana Mayerly Bernal Zapata		
ANALISIS DE EFECTIVIDAD			

La Oficina de Control Interno da como inefectivas las acciones de mejora, teniendo en cuenta la No Conformidad Nro. 6 Debilidades en la documentación, aprobación, comunicación y alineación de la Política del MSPI con los objetivos institucionales.

OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025.

(…)" Conforme a lo manifestado, la No Conformidad No. 6 planteada no aplica en los términos expuestos, toda vez que la Entidad sí cuenta con los instrumentos documentales requeridos que dan cumplimiento al MSPI y a la norma ISO/IEC 27001:2022. En consecuencia, se solicita que la observación sea reclasificada como Conformidad con oportunidad de mejora, en lugar de no conformidad.
De igual manera, se precisa que las acciones formuladas fueron ejecutadas de forma efectiva y eficaz, tal como se evidencia a continuación:

- *Actualización de la Política de Seguridad de la Información: Durante la vigencia 2024 se adelantó la actualización de la Política de Seguridad y Privacidad de la Información. Esta actualización fue presentada para aprobación en la sesión 3 del Comité Institucional de Gestión y Desempeño, realizada el 7 de octubre de 2024, publicada el 29 de octubre de 2024 y socializada en la Entidad el 26 de febrero de 2025.*
- *Seguimiento a la implementación de la Política de Seguridad de la Información: Tal como se evidenció en el proceso de auditoría (requerimiento entregado el 15 de julio de 2024, carpeta "Monitoreo del MSPI" – subcarpeta "Implementación de la Política"), se realiza seguimiento trimestral desde la vigencia 2024.*
- *Publicación del procedimiento de administración de riesgos: Durante la vigencia 2024 se creó el DEST–P-011 Procedimiento Administración de Riesgos de Seguridad de la Información, publicado en el SIG el 19 de septiembre de 2024 y socializado el 19 de diciembre de 2024.*
- *Formulación del Mapa de Riesgos de Seguridad de la Información: Se llevaron a cabo mesas técnicas con cada dependencia de la Entidad durante 2024 para identificar riesgos asociados a activos de información. Las evidencias fueron remitidas en la respuesta al requerimiento de auditoría el 3 de julio de 2025 (carpeta "1. Adopción de los requisitos del MSPI en los procesos de la Entidad"). El resultado de este ejercicio fue el Mapa de Riesgos de la Entidad, publicado en la página web de la ANT el 3 de febrero de 2025.*
- *Implementación de herramienta para gestión de riesgos: Se adoptó la herramienta DEST-F-004 Mapa de Riesgos de Seguridad de la Información V2, publicada en el SIG. Esta herramienta permite registrar activos de información, identificar vulnerabilidades y amenazas, calcular el riesgo inherente y residual, verificar controles conforme al Anexo A de la ISO 27001, y establecer acciones preventivas. Asimismo, incluye un anexo para registrar la materialización de riesgos y planes de acción asociados.*

Con lo anterior, se evidencia que las acciones implementadas atendieron directamente la causa raíz identificada en la auditoría, logrando su mitigación en su totalidad

Conclusión SSIT

De acuerdo con las evidencias presentadas, las acciones implementadas atendieron de manera integral la causa raíz identificada, logrando la actualización, aprobación, publicación y socialización de la Política de Seguridad de la Información; la formalización del procedimiento de administración de riesgos; la formulación y publicación del mapa de riesgos institucional; y la implementación de una herramienta de gestión y seguimiento. Estos resultados demuestran que las medidas adoptadas fueron eficaces y contribuyeron al fortalecimiento del MSPI, en cumplimiento con la norma ISO/IEC 27001:2022.

En este sentido, no resulta procedente calificarlas como inefectivas, sino reconocer que las acciones de mejora fueron ejecutadas con efectividad y eficacia, mitigando en su totalidad la observación planteada.
." (…).

CONCLUSIÓN EQUIPO AUDITOR

La Oficina de Control Interno observó que, pese a los avances evidenciados en la actualización, publicación y socialización de la Política de Seguridad de la Información, así como en la adopción de instrumentos complementarios, las acciones implementadas resultan inefectivas dado que, persisten vacíos en la alineación de la Política con los objetivos estratégicos institucionales y la efectividad en su comunicación a todos los niveles, lo que limita su capacidad de orientar de forma integral la gestión del MSPI. Por lo anterior se mantiene la inefectividad conforme a la No Conformidad Nro. 6.

Actividad Origen	Informe Seguimiento Gestión de Riesgos de Gestión e Informáticos		
No. Hallazgo	R1	**Código Acción (es)**	AMI-264
Causa Raíz	Deficiencias en la cantidad de controles formulados, relacionadas con la frecuencia, documentación y evidencias.		
Acción de mejora	➢ Formulación del mapa de riesgos de seguridad de la información fortaleciendo las acciones de control y preventivas		
Estado Efectividad	Efectiva ( ) Inefectiva (**X**)		
Auditor Verificador	Diana Mayerly Bernal Zapata		
ANALISIS DE EFECTIVIDAD			
La Oficina de Control Interno da como inefectivas las acciones de mejora, teniendo en cuenta la No Conformidad Nro. 9. Debilidades en la planificación e implementación de controles.			

OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025.

(…)" Con relación a la No Conformidad No. 9, se evidencia que la entidad cuenta con instrumentos normativos y operativos que soportan la gestión de riesgos y la implementación de controles de seguridad de la información. En consecuencia, solicitamos que dicha no conformidad sea reevaluada, considerando la evidencia documental y la integración de los planes y procedimientos existentes.

Acciones ejecutadas:

- *Se realizaron mesas técnicas con las dependencias durante 2024 para identificar riesgos asociados a los activos de información, consolidando la información en el Mapa de Riesgos de Seguridad de la Información, publicado en la página web institucional el 3 de febrero de 2025.*
- *Se remitieron las evidencias al requerimiento de auditoría el 3 de julio de 2025, en la carpeta 1. Adopción de los requisitos del MSPI en los procesos de la entidad, subcarpeta 1.3 Gestión de riesgos.*

Conclusión SSIT

Las acciones implementadas resultaron efectivas y suficientes, al permitir estructurar formalmente la gestión de riesgos de seguridad de la información y fortalecer los mecanismos de control preventivo, en cumplimiento de la norma ISO/IEC 27001:2022." (…).

CONCLUSIÓN EQUIPO AUDITOR

Tras el análisis de las observaciones allegadas por la SSIT, la Oficina de Control Interno concluye que las acciones de mejora implementadas resultan inefectivas, dado que, aunque existen documentos como el Plan de Cierre de Brechas, el Procedimiento de Administración de Riesgos, el Mapa y el Plan de Tratamiento, persisten debilidades en la definición de periodicidad, responsables y acciones preventivas específicas, así como en la trazabilidad y verificación de los controles; situación que limita la planificación e implementación establecida en el numeral 8.1 del MSPI. Por lo anterior se mantiene la inefectividad conforme a la No Conformidad Nro. 9.

5. EVALUACIÓN DEL RIESGO

La política evidencia un enfoque integral al incorporar explícitamente la gestión de riesgos de seguridad de la información como uno de sus pilares, alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC. Esta gestión es presentada como una herramienta esencial para proteger la confidencialidad, integridad y disponibilidad de los activos de información.

Conforme a lo anterior, se identificaron las siguientes fortalezas:

- Respaldo a la implementación del SGSI y a la gestión de riesgos, incluyendo provisión de recursos técnicos, humanos y financieros.
- La política contempla revisiones periódicas y exige una reiniciación del ciclo PHVA cada tres años, lo cual fortalece la identificación y mitigación continua de riesgos emergentes.

A continuación, se registran las observaciones frente a los riesgos identificados en el mapa de Gestión y Mapa de Riesgos de Seguridad de la Información de la Agencia con relación a las actividades de Seguridad de la Información:

Nro.	Tipo de Riesgo	Riesgo	Observaciones
R14	**Riesgo de Gestión**	Incumplimiento en la implementación del MSPI de la estrategia de Gobierno Digital.	La materialización del riesgo se estableció a partir de los resultados observados en la No Conformidad Nro. 1 Debilidades en el avance de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).
	<u>OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025.</u> *(…) "No se considera que el Riesgo de Gestión R14 se haya materializado, toda vez que la entidad no presenta incumplimiento en la implementación del MSPI. El nivel de madurez actual refleja el avance progresivo esperado en el marco de los lineamientos del MinTIC y orienta las acciones de mejora mediante la ejecución del Plan de cierre de brechas. Cabe precisar que los instrumentos del MinTIC no definen un porcentaje mínimo de avance anual, sino que plantean un proceso gradual y contextualizado. En consecuencia, lo evidenciado corresponde a una etapa natural de fortalecimiento y no a un evento adverso que implique impacto real sobre la seguridad o la privacidad de la información.* *En consecuencia, la calificación del riesgo como "materializado" carece de sustento técnico, dado que no existe evidencia de un evento adverso o incumplimiento real, sino un proceso natural de maduración del modelo en curso" (…)* **<u>CONCLUSION EQUIPO AUDITOR</u>** Teniendo en cuenta las observaciones por parte de las SSIT y con base en las evidencias recolectadas, la OCI concluye que las No Conformidades son consistentes con una alerta de incremento en la probabilidad de ocurrencia del riesgo, mas no con una materialización.		

R23	**Riesgo de Seguridad de la Información**	Pérdida de Integridad y la confidencialidad de los datos almacenados y gestionados en los sistemas de información de la entidad utilizados en los diferentes procesos, debido a bajo conocimiento de los conceptos y procedimientos de seguridad de la información.	El riesgo se considera materializado, ya que se reporta uso compartido de credenciales y fallas en la protección de información, lo cual compromete integridad y confidencialidad. No Conformidad Nro. 8.
	<u>OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025.</u> *(…) "No se considera que el Riesgo de Seguridad de la Información R23 esté materializado, dado que no se ha evidenciado pérdida real de la integridad ni de la confidencialidad de los datos institucionales. Las situaciones observadas, como el uso compartido de credenciales o fallas puntuales en los controles, corresponden a vulnerabilidades que aumentan la probabilidad de ocurrencia, pero no constituyen un evento de materialización del riesgo. En este sentido, la entidad viene ejecutando las acciones de control 28 y 29, relacionadas con la capacitación en la Política y Lineamientos de Seguridad de la Información, orientadas a mitigar estas prácticas y fortalecer la cultura de protección de la información.* *Adicionalmente, se precisa que a la fecha no se ha reportado incidente de seguridad o evento* que evidencie la materialización del riesgo R23." (…) **<u>CONCLUSION EQUIPO AUDITOR</u>** Teniendo en cuenta las observaciones por parte de las SSIT y con base en las evidencias recolectadas, la OCI concluye que las No Conformidades son consistentes con una alerta de incremento en la probabilidad de ocurrencia del riesgo, mas no con una materialización.		
R27	**Riesgo de Seguridad de la Información**	Pérdida la confidencialidad de la información por uso ilegítimo de datos personales (utilización de datos para finalidades distintas a las autorizadas por el titular).	El riesgo se materializa por debilidades en el control de acceso a la información, además del uso indebido de credenciales de acuerdo con la No Conformidad Nro. 13.
	<u>OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025.</u> *(…)"* E*l riesgo de Seguridad de la Información R27 no se ha materializado, dado que no se evidencia exposición malintencionada de la información, ni pérdida de la integridad de la misma. A pesar del uso inadecuado de credenciales, no existen pruebas técnicas que demuestren que dichas prácticas se hayan utilizado con la finalidad de causar afectación, exponer intencionalmente datos, modificar información en detrimento de la entidad o de los titulares, ni que se hayan empleado para finalidades distintas a las autorizadas por estos.* *En este sentido, las situaciones reportadas corresponden a vulnerabilidades que incrementan la probabilidad de ocurrencia del riesgo, pero no constituyen evidencia de un impacto real sobre la confidencialidad o integridad de la información.* ***Por lo tanto, no es posible concluir la materialización***		

	del riesgo partiendo de supuestos, sino únicamente con base en hechos comprobados y soportados técnicamente" (…) **CONCLUSION EQUIPO AUDITOR** Teniendo en cuenta las observaciones por parte de las SSIT y con base en las evidencias recolectadas la OCI concluye que las No Conformidades son consistentes con una alerta de incremento en la probabilidad de ocurrencia del riesgo, mas no con una materialización.		
UGT Pasto			
R67	**Riesgo de Seguridad de la Información**	Pérdida de la confidencialidad de la información de la entidad, debido a bajo conocimiento de los conceptos y procedimientos de seguridad de la información.	Riesgo materializado parcialmente, en concordancia con los resultados de la encuesta (falta de apropiación de lineamientos, baja asistencia a capacitaciones), lo que afecta directamente la protección de la información de acuerdo con la No Conformidad Nro. 1 y No Conformidad Nro.13.
	OBSERVACIONES ALLEGADAS POR LA SSIT MEDIANTE CORREO ELECTRÓNICO DEL 02/09/2025. *(…) "Se considera que el Riesgo de Seguridad de la Información R67 no se ha materializado.* *Los resultados de la encuesta únicamente reflejan oportunidades de mejora en la apropiación de los lineamientos y en la asistencia a las capacitaciones, pero no constituyen evidencia técnica de un impacto real sobre la confidencialidad de la información.* *Cabe precisar que una baja percepción de conocimiento o asistencia limitada a espacios formativos incrementa la probabilidad de ocurrencia del riesgo, al dejar en evidencia vulnerabilidades culturales y de práctica organizacional. Sin embargo, no puede ser interpretado como una materialización parcial del riesgo, ya que no se demuestra pérdida, exposición indebida o uso ilegítimo de información institucional.* *En este sentido, se solicita que tales hallazgos sean tratados como insumos para fortalecer los controles de concientización y formación, pero no como una evidencia de materialización del riesgo." (…)* **CONCLUSION EQUIPO AUDITOR** Teniendo en cuenta las observaciones por parte de las SSIT y con base en las evidencias recolectadas, la OCI concluye que las No Conformidades son consistentes con una alerta de incremento en la probabilidad de ocurrencia del riesgo, mas no con una materialización.		

Tabla 7. 7 *Evaluación del Riesgo*
Fuente: *No conformidades en el Informe*

6. CONCLUSIONES

Las conclusiones presentadas a continuación recogen de manera integral los hallazgos obtenidos durante la auditoría interna al Modelo de Seguridad y Privacidad de la Información (MSPI) de la Agencia Nacional de Tierras. Su propósito es sintetizar el nivel de cumplimiento identificado frente a los criterios de auditoría, destacar los aspectos positivos alcanzados por la entidad y señalar las principales brechas y oportunidades de mejora que requieren atención prioritaria para fortalecer la gestión de la seguridad y privacidad de la información, en coherencia con los objetivos estratégicos institucionales y el marco normativo aplicable.

Con el fin de facilitar la comprensión global de los hallazgos, tanto de conformidad como de no conformidad, estos se presentan conforme a los cinco componentes que integran el Modelo Estándar de Control Interno – MECI: (i) ambiente de control, (ii) evaluación del riesgo, (iii) actividades de control, (iv) información y comunicación, y (v) actividades de monitoreo. Esta segmentación permite evidenciar de manera estructurada las fortalezas y debilidades observadas en la implementación del MSPI y su articulación con el sistema de control interno institucional.

A continuación, se presenta la consolidación de resultados por hallazgos observados:

Componente MECI	Conformidades	No Conformidades
1. Ambiente de Control	**C2**. Inclusión de funciones relacionadas con seguridad y privacidad de la información en el Comité Institucional de Gestión y Desempeño. **C4.** Cumplimiento en la articulación de roles institucionales y en la delegación formal del responsable de seguridad y privacidad de la información.	**NC5.** Debilidades en el liderazgo y compromiso del Comité Institucional de Gestión y Desempeño frente al MSPI. **NC6.** Debilidades en la documentación, aprobación, comunicación y alineación de la Política del MSPI con los objetivos institucionales. **NC7.** Debilidades en el esquema institucional de roles y responsabilidades para la implementación del MSPI.
2. Evaluación del Riesgo	**C5.** Cumplimiento en la Identificación de activos de información e infraestructura crítica. **C6.** Cumplimiento en la valoración de los riesgos de seguridad de la información. **C8.** Cumplimiento en la formulación del Plan de tratamiento de los riesgos de seguridad de la información.	**NC2.** Debilidades en la definición específica del contexto de la entidad conforme al MSPI. **NC3.** Debilidades en la determinación de partes interesadas relevantes para la Seguridad de la Información. **NC4.** Debilidades en la definición formal y aprobación del alcance del MSPI.

Componente MECI	Conformidades	No Conformidades
3. Actividades de Control	**C3.** Cumplimiento en Procedimientos de Seguridad de la Información.	**NC1**. Debilidades en el avance de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI). **NC8.** Debilidades en el plan de comunicación, capacitación, sensibilización y concientización. **NC9.** Debilidades en la Planificación e implementación de controles. **NC13.** Debilidades en la implementación de Procedimientos de Seguridad de la Información UGT Pasto.
4. Información y Comunicación	**C1.** Aplicación y trazabilidad del diagnóstico del MSPI como insumo para la planificación y el seguimiento del modelo.	—
5. Actividades de Monitoreo	**C7.** Disponibilidad y suficiencia de recursos para el MSPI. **C9.** Cumplimiento del requisito de auditoría interna del MSPI con planificación y aprobación formal.	**NC10**. Debilidades en el seguimiento, medición, análisis y evaluación del MSPI. **NC11.** Debilidades en la revisión por la dirección del MSPI. **NC12.** Debilidades en el Plan Anual de Mejora del MSPI.

Tabla 8. 8 *Hallazgos conforme estructura MECI*
Fuente: Informe Auditoría MSPI

En la verificación realizada sobre la efectividad de las acciones implementadas frente a los hallazgos identificados en evaluaciones anteriores, se constató que dichas acciones fueron ejecutadas; no obstante, se evidenció que no resultaron efectivas, ya que no corrigieron la causa raíz de los hallazgos originales. En este sentido, se hace necesario reformular el plan de mejoramiento, de manera que las nuevas medidas propuestas permitan una solución integral y sostenible a las debilidades observadas.

En la evaluación del riesgo se constató que la Agencia Nacional de Tierras dispone de un marco metodológico formal para la identificación, análisis y valoración de riesgos de seguridad de la información, sustentado en los instrumentos institucionales y alineado con el MIPG y con estándares internacionales. No obstante, se concluye que las No Conformidades son consistentes con una alerta de incremento en la probabilidad de ocurrencia de los riesgos (R14, R23, R27, R67), mas no una materialización.

7. RECOMENDACIONES

En el marco de la auditoría, además de las no conformidades identificadas, se emitieron recomendaciones derivadas de las conformidades observadas. Estas recomendaciones corresponden a sugerencias formuladas por el equipo auditor con base en su experiencia y en las prácticas de referencia en la materia, orientadas a señalar oportunidades de mejora sobre aspectos que cumplen con los requisitos establecidos.

Es importante precisar que las recomendaciones no responden a incumplimientos normativos, sino a observaciones realizadas en procesos que ya presentan conformidad. En este sentido, la implementación de planes de mejoramiento asociados a estas recomendaciones es discrecional para el área auditada, de acuerdo con su priorización y capacidades institucionales.

A continuación, se relacionan las recomendaciones formuladas por el equipo auditor, derivadas de las conformidades observadas, en atención a las oportunidades de mejora identificadas:

Componente MECI	Recomendaciones Propuestas (con numeral MSPI)	Finalidad
1. Ambiente de Control	**MSPI 7.2.1.** Expedir un acto administrativo complementario que actualice la Resolución 183 de 2018 para incluir explícitamente las funciones del CIGD sobre el MSPI. **MSPI 7.2.1.** Socializar internamente el rol del CIGD y garantizar la trazabilidad en actas. **MSPI 7.3.6 y 7.3.7.** Ajustar el Manual INTI-M-001 y la Política INTI-008 para consolidar roles, responsabilidades y lineamientos de reporte ante el CIGD.	Asegurar gobernanza, trazabilidad institucional y apropiación de roles para la sostenibilidad del modelo.
2. Evaluación del Riesgo	**MSPI 7.3.2.** Fortalecer la articulación entre el autodiagnóstico y la matriz de riesgos, con trazabilidad en las decisiones de aceptación. **MSPI 7.3.2.** Documentar y aprobar una matriz de apetito y tolerancia al riesgo. **MSPI 7.3.2.** Implementar herramientas tecnológicas de gestión de riesgos para mayor trazabilidad.	Fortalecer la gestión integral de riesgos y la toma de decisiones estratégicas con base en evidencia.
3. Actividades de Control	**MSPI 7.3.8.** Establecer indicadores de la Política de Seguridad de la Información y hacer seguimiento diferenciado por dominio de seguridad. **MSPI 7.3.9.** Fortalecer el procedimiento GINFO-P-011 Gestión de Incidentes con métricas de desempeño y trazabilidad documental.	Incrementar la efectividad operativa de los controles y su alineación con la gestión institucional del MSPI.

Componente MECI	Recomendaciones Propuestas (con numeral MSPI)	Finalidad
	MSPI 7.3.10. Alinear la política de protección de datos personales con el MSPI y RNBD actualizado. **MSPI 7.4.1.** Incluir la identificación de activos en procesos de gestión del cambio y proyectos tecnológicos, con trazabilidad al mapa de riesgos.	
4. Información y Comunicación	**MSPI 7.4.2.** Ampliar la cobertura de capacitaciones al 100% de los funcionarios, con contenidos diferenciados por rol y nivel de riesgo. **MSPI 7.4.2.** Incluir actividades dirigidas a partes interesadas externas (proveedores, aliados estratégicos). **MSPI 7.4.2.** Implementar encuestas de percepción institucional y reportes consolidados de apropiación.	Garantizar la apropiación institucional y externa del MSPI, así como evaluar la efectividad de la comunicación.
5. Actividades de Monitoreo	**MSPI 7.5.1 y 7.5.4.** Formalizar los informes de seguimiento del MSPI, con responsable, fechas, constancia de remisión y aprobación del Oficial de Seguridad. **MSPI 9.1.2.** Incluir en el Plan Anual de Auditoría actividades específicas de revisión del MSPI y seguridad digital. - **MSPI 7.3.6 / 7.3.7.** Incorporar reportes periódicos del Oficial de Seguridad al CIGD con indicadores y resultados de auditorías.	Consolidar la trazabilidad, la retroalimentación institucional y la mejora continua en la gestión del MSPI.

Tabla 9. *Recomendaciones conforme estructura MECI*
Fuente: Informe Auditoría MSPI

1. ANEXOS

En esta actividad de aseguramiento no se generaron anexos para disposición del área auditada.

Aprobó,

(Documento físico firmado)
ARIEL LEONEL MELO
Jefe Oficina de Control Interno

Elaboró,

(Documento físico firmado)
DIANA MAYERLY BERNAL ZAPATA
Auditor, Contratista Oficina de Control Interno

(Documento físico firmado)
LILA MARIA GUZMÁN
Auditor, Gestor T1 G10 Oficina de Control Interno

Septiembre, 4 del 2025.