PLAN DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

DIRECCIÓN DE GESTION DEL ORDENAMIENTO SOCIAL DE LA PROPIEDAD

SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS

CONTENIDO

1. INTRODUCCIÓN

En cumplimiento de lo establecido en el Decreto 612 de 2018, mediante el cual se definen los lineamientos para la integración de los planes institucionales y estratégicos de las entidades públicas en el marco del Modelo Integrado de Planeación y Gestión – MIPG, la entidad formula el Plan de Seguridad y Privacidad de la Información, como un instrumento de planeación que orienta la gestión integral de la seguridad de la información y la protección de los datos personales.

Este Plan se articula con el Modelo de Seguridad y Privacidad de la Información – MSPI, liderado por el Ministerio de Tecnologías de la Información y las Comunicaciones, y adopta las mejores prácticas establecidas en la norma internacional ISO/IEC 27001, con el fin de establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI) basado en riesgos. De esta manera, se garantiza la confidencialidad, integridad y disponibilidad de la información que soporta el cumplimiento de la misión institucional y la prestación de los servicios a la ciudadanía.

El Plan de Seguridad y Privacidad de la Información se concibe como un componente transversal del MIPG, articulado con los procesos estratégicos, misionales, de apoyo y de evaluación, y alineado con la gestión del riesgo institucional, el control interno y la transformación digital. Asimismo, incorpora un enfoque preventivo y proactivo frente a los riesgos de seguridad de la información, ciberseguridad y privacidad, fortaleciendo la capacidad de la entidad para prevenir, detectar y responder a incidentes que puedan afectar sus activos de información.

A través de la ejecución de las acciones definidas en este Plan, la entidad reafirma su compromiso con el cumplimiento normativo, la protección de los derechos de los titulares de la información, la confianza digital y la mejora continua, contribuyendo al fortalecimiento de la gestión pública, la transparencia y la eficiencia institucional.

2. DEFINICIONES

• Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

• Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

• Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

• Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos

que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

• Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

• Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

• Autenticidad: La entidad que accede al activo de información está verificada y es la que declara ser.

• Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

• Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

• Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

• Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada. Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

• Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000).

• Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo. Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

• Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

• Evitación del riesgo: Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

• Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

• Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

• Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

• Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

• Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

• Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000). Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

• Información: Conjunto de datos que tienen un significado.

• Integridad: Propiedad de la información relativa a su exactitud y completitud.

• Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

• Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.

• Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

• Parte interesada: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

• Probabilidad: Posibilidad de que una amenaza se materialice.

• Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

• Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado.

• Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

• Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

• Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular.

• Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

• Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. Riesgo Positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

• Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

• Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera.

• Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

• Tolerancia al riesgo: son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

• Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

• Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

• Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

• Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

3. OBJETIVOS

3.1. Objetivo general

Establecer las actividades del Plan de Gestión de Seguridad y Privacidad de la Información que permitan mantener la seguridad y privacidad de la información en los procesos de la Agencia Nacional de tierras, articulado con el Sistema de Gestión de Seguridad de la Información (SGSI) y teniendo en cuenta los requerimientos y actividades contempladas en el Modelo de Seguridad y Privacidad de la Información MSPI de la estrategia de Gobierno Digital, los requerimientos del negocio de la ANT, y el cumplimiento a las disposiciones legales vigentes nacionales e internacionales

3.2. Objetivos específicos

- Implementar y fortalecer la gestión de la seguridad y privacidad de la información en los procesos de la Agencia Nacional de Tierras, en articulación con el Sistema de Gestión de Seguridad de la Información (SGSI) y el Modelo de Seguridad y Privacidad de la Información (MSPI).

- Gestionar los riesgos de seguridad y privacidad de la información, mediante la identificación, análisis, tratamiento y seguimiento de los riesgos asociados a los activos de información.

- Definir y ejecutar controles orientados a proteger la confidencialidad, integridad y disponibilidad de la información, asegurando el cumplimiento de los requisitos legales y normativos aplicables.

- Fortalecer la cultura organizacional en seguridad y privacidad de la información, a través de acciones de cambio, capacitación, sensibilización y comunicación.

4. ALCANCE

El presente Plan de gestión aplica para los procesos de la Agencia Nacional de Tierras, con el fin de dar cumplimiento a la implementación de la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información basado en la NTC/IEC ISO 27001:2013 y la Política de Seguridad Digital.

5. BASE LEGAL

- Constitución Política de Colombia. Artículos 15, 20, 23 y 74.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- • Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC- Se crea la agencia Nacional de espectro y se dictan otras disposiciones.
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley 527 de 1999. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Decreto 338 de 2022. Por el cual se adiciona el Titulo 21 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
- Decreto 767 de 2022. Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 88 de 2022. Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea.
- Decreto 620 de 2020. Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los

literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

- Decreto 2106 de 2019. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- Decreto 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 2364 de 2012. Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Resolución 0448 de 2022. Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se deroga la resolución 2256 de 2020.
- Resolución 746 de 2022. Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021
- Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital
- Resolución 1519 de 2020. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- Resolución 924 de 2020. Por la cual se actualiza la Política de Tratamiento de Datos Personales del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 2007 de 2018.

- Resolución 0860 de 2025, "por la cual se actualiza el Modelo Integrado de Gestión (MIG) y el Sistema Integrado de Gestión (SIG) del Ministerio de Tecnologías de la Información y las Comunicaciones/Fondo Único de Tecnologías de la Información y las Comunicaciones, y se deroga la Resolución 4870 de 2023 y sus modificatorias".
- Resolución 02277 de 2025, "por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia".
- CONPES 3995 de 2020. Confianza y Seguridad Digital.
- CONPES 3854 de 2017. Política Nacional de Seguridad digital
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 4069 de 2022. Política Nacional de Ciencia, tecnología e innovación 2022 – 2031
- Directiva 26 de 2020. Diligenciamiento de la información en el índice de transparencia y acceso a la información – ITA – de conformidad con las disposiciones el artículo 23 de la ley 1712 de 2014.

6. RECURSOS.

- ESTRATÉGICOS: Documentación asociada a Políticas, lineamientos, procedimientos y planes de seguridad de la Información de la ANT.

- HUMANOS: La Subdirección de Sistemas de Información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua, la Dirección de Gestión del Ordenamiento Social de la Propiedad, la Secretaría General, la Subdirección de Talento Humano, los líderes de los procesos y la Oficina de Control Interno, apoyaran operativa y técnicamente en la atención y supervisión necesaria según el rol designado.

- SOTWARE: Equipos virtualizados, herramientas y software para la seguridad de TI, asi como los activos de información inventariados.

- FÍSICOS: Infraestructura de TI, redes, comunicaciones y controles de acceso físico.

7. RESPONSABLES

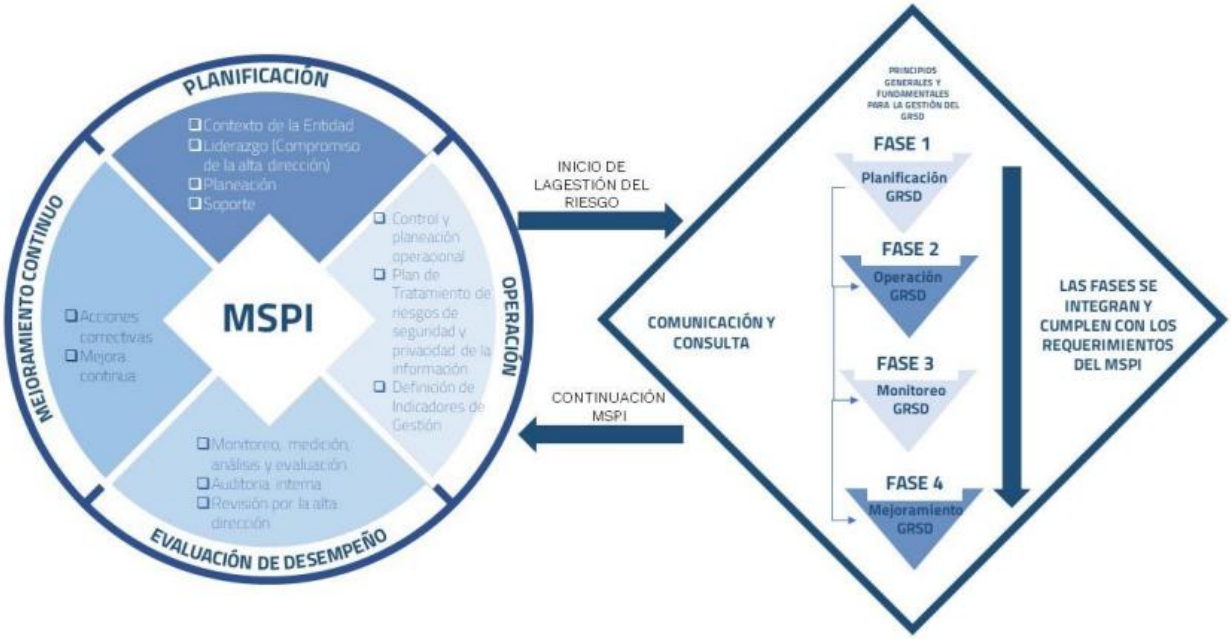
La responsabilidad de las acciones relacionadas con los procesos, políticas y lineamientos de Seguridad de la Información está enmarcada en:

- Dirección de Gestión del Ordenamiento Social de la Propiedad.
- Subdirección de Sistemas de Información de Tierras.
- Equipo de Infraestructura y Soporte Tecnológico – EIST de la Secretaria General.
- Mesa Técnica de TI.
- Áreas de procesos.

• Subdirección de Talento Humano.
• Equipo de Seguridad de la Información.

8. METODOLOGÍA IMPLEMENTACIÓN MODELO DE SEGURIDAD

Ilustración 1 Ciclo del Modelo de Seguridad y Privacidad de la Información



Fuente: MinTIC. Anexo 1 Modelo de Seguridad y Privacidad MSPI, (2021).

8.1. Fase I (Diagnóstico)

Objetivo: Identificar el estado de la ANT con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información - MSPI.

Esta fase permite identificar el estado actual de la ANT (Análisis GAP) con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, el resultado de este diagnóstico sirve para dar inicio al MSPI.

8.1.1. SITUACIÓN ACTUAL DE LA ANT

A continuación, se presenta el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información como parte de la Política Nacional de Gobierno Digital, basada en la ISO/EC 27001:2022:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	57	100	EFECTIVO
A.6	CONTROLES DE PERSONAS	63	100	GESTIONADO
A.7	CONTROLES FÍSICOS	49	100	EFECTIVO
A.8	CONTROLES TECNOLÓGICOS	63	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		58	100	EFECTIVO

Tabla 1. Resultados de evaluación de efectividad de controles.
Fuente: Modelo de Seguridad y Privacidad de la Información – MSPI ANT Portada.

La tabla de Evaluación de Efectividad de Controles evidencia el nivel actual de madurez alcanzado en cada dominio evaluado del Modelo de Seguridad y Privacidad de la Información. Los resultados muestran desempeños diferenciados entre los componentes analizados: el dominio Organizacional y el dominio Tecnológico presentan los puntajes más altos con 63 puntos, lo que refleja avances significativos en la definición de lineamientos, estructuras administrativas y la existencia de controles tecnológicos y de ciberseguridad en operación. Por su parte, el dominio de Personas registró 49 puntos, indicando la necesidad de fortalecer la cultura institucional en seguridad, la capacitación continua y el aseguramiento de competencias del personal. El conjunto global de dominios permitió calcular un promedio de evaluación de controles de 58 puntos frente a una calificación objetivo de 100, lo que demuestra la existencia de bases consolidadas, pero también de una brecha sustancial que debe cerrarse mediante la planificación de acciones de mejora, automatización de controles y fortalecimiento de procesos operativos y de gestión.
A continuación, se presenta el avance actual para cada componente según el PHVA

AÑO	COMPONENTE (PHVA)	CLAUSULAS	% de Avance Actual	% Avance Esperado
2025	Planificación	Contexto de la organización	8%	14%
		Liderazgo	11%	14%
		Planificación	7%	14%
		Soporte	10%	14%
	Implementación	Operación	10%	16%
	Evaluación de Desempeño	Evaluación del desempeño	7%	14%
	Mejora Continua	Mejora	6%	14%
TOTAL			59%	100%

Tabla 2. Avance actual del componente PHVA
Fuente: Portada Instrumento de Autodiagnóstico MSPI 2025

El análisis de cumplimiento del sistema de gestión para el año 2025, estructurado bajo el ciclo PHVA, consolidó un porcentaje de avance actual del 59% en comparación con el nivel objetivo de 100%.

En el componente de Planificación, los indicadores de cumplimiento por cláusula fueron: contexto de la organización (8%), liderazgo (11%), planificación (7%) y soporte (10%), todos con un avance esperado del 14%.

El componente de Implementación presentó un 10% en la cláusula de operación frente al objetivo del 16%. Respecto a Evaluación del Desempeño, la cláusula correspondiente registró un 7%, mientras que, en Mejora Continua, el cumplimiento alcanzó el 6%, cada uno con una meta del 14%.

La brecha identificada demuestra que el desarrollo del Sistema de Gestión de Seguridad de la Información se concentra en etapas iniciales de planeación y ejecución, mientras que los mecanismos de monitoreo, análisis, retroalimentación y mejora aún no se encuentran institucionalizados. Estos resultados servirán como insumo para la priorización de acciones y el diseño del plan de fortalecimiento del sistema.

Fuente: Portada Instrumento de Autodiagnóstico MSPI 2025 - anexo ISO27001:2022

8.2. Fase II Implementación Plan de Seguridad y Privacidad de la Información

GESTIÓN	ACTIVIDADES	FECHA INICIO	FECHA FIN
Activos de Información	Revisión y actualización si aplica, del procedimiento y el instructivo para la valoración de activos de información.	16/02/2026	31/03/2026
	Actualización Matriz de Activos de Información con su respectiva valoración, mediante el desarrollo de mesas técnicas	01/04/2026	30/06/2026
	Revisión y aprobación de la matriz de activos de información de la entidad	01/10/2026	30/10/2026
	Publicación del INTI-F-020 REGISTRO ACTIVOS DE INFORMACIÓN y el INTI-F-022 INFORMACIÓN CLASIFICADA Y RESERVADA	01/10/2026	30/10/2026
Gestión de Riesgos	Revisión y actualización si aplica, del procedimiento para administración de riesgos de seguridad de la información	10/03/2026	31/05/2026
	Identificación y valoración de riesgos sobre los activos de información en la entidad (vigencia 2026)	01/07/2026	30/11/2026
	Establecimiento de acciones preventivas vigencia 2027 - Aceptación perfiles de riesgo	01/07/2026	30/11/2026
	Medición y verificación de los controles de seguridad de acuerdo al proceso de identificación de riesgos de seguridad de la información	01/07/2026	30/11/2026
	Consolidación y aprobación del mapa de riegos para publicación.	01/10/2026	31/12/2026
Revisión de los controles de la norma ISO 27001	Ejercicios trimestrales de inspecciones a controles de acuerdo con SoA	16/02/2026	31/12/2026
	Seguimiento a hallazgos detectados en las inspecciones	16/02/2026	31/12/2026
Gestión de Incidentes de Seguridad y Privacidad de la Información	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	01/02/2026	30/06/2026
	Gestionar los incidentes y/o ataques de Seguridad de la Información identificados	01/01/2026	31/12/2026
	CSIRT - Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno	01/01/2026	31/12/2026
	Revisar lecciones aprendidas de la gestión de eventos e incidentes y definir requerimientos de actualización del procedimiento de Gestión de incidentes de seguridad de la información y sus herramientas	01/03/2026	31/12/2026
	Realizar seguimiento a los informes de eventos asociados a SGSI	01/01/2026	31/12/2026
Vulnerabilidades	Socializar la política de Gestión de Vulnerabilidades y sus anexos	01/02/2026	30/04/2026
	Definir los lineamientos, mecanismos y el alcance para la realización de pruebas de vulnerabilidades y pentest	01/03/2026	31/12/2026
	Ejecución de las pruebas de vulnerabilidades y pentest (HE)	01/01/2026	31/12/2026
	Realizar seguimiento a los informes de vulnerabilidades asociados a SGSI	01/03/2026	31/12/2026

GESTIÓN	ACTIVIDADES	FECHA INICIO	FECHA FIN
	Seguimiento al plan de remediación de acuerdo con las vulnerabilidades identificadas	01/03/2026	31/12/2026
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	01/02/2026	31/03/2026
	Ejecutar el del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	01/02/2026	31/12/2026
	Reporte trimestral de gestión del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	01/03/2026	31/12/2026
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Actualizar la Matriz de verificación de Requisitos legales de Seguridad de la Información	01/02/2026	31/12/2026
	Establecer acciones que dan cumplimiento a los Requisitos legales de Seguridad de la Información en la entidad	01/04/2026	31/12/2026
	Publicar y Socializar la Matriz de verificación de Requisitos legales de Seguridad de la Información	01/06/2026	31/31/2026
Plan de Continuidad del Negocio	Actualización del Análisis de Impacto de la operación 2026	16/02/2026	30/06/2026
	Seguimiento de Riesgos de Interrupción	16/02/2026	15/12/2026
	Actualización de Documentación de Estrategias de Continuidad	16/02/2026	15/12/2026
	Seguimiento Implementación Estrategias de Continuidad	16/02/2026	15/12/2026
	Documentación del Plan de continuidad de la Operación actualizado 2026	16/02/2026	15/12/2026
	Socialización y capacitación Plan de Continuidad, Plan de Recuperación de Desastres y Análisis de Impacto del Negocio	01/03/2026	31/12/2026
Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información	01/04/2026	31/12/2026
	Revisar y alinear la documentación del SGSI de la entidad al MSPI, de acuerdo con la Normatividad vigente.	01/04/2026	31/12/2026
	Realizar el análisis de brechas en la implementación de controles de seguridad física por parte de los colaboradores de la entidad	01/04/2026	31/12/2026
	Implementar la política de seguridad y privacidad de la información	01/03/2026	31/12/2026
	Comunicar la política de seguridad y privacidad de la información	01/03/2026	31/12/2026
Gestión de datos personales y derechos de autor	Recolectar y revisar bases de datos	16/02/2026	30/06/2026
	Registro y actualización de las bases de datos	16/02/2026	31/08/2026
	Verificación de cumplimiento de derechos de autor y propiedad intelectual	16/02/2026	31/12/2026
Oportunidades de mejoras SGSI	Reporte del estado de las Acciones Correctivas, correcciones y Oportunidades de Mejora	01/05/2026	31/12/2026
	Realizar seguimiento a las oportunidades de mejora producto de revisiones internas y externas a los Procesos	01/05/2026	31/12/2026

GESTIÓN	ACTIVIDADES	FECHA INICIO	FECHA FIN
Documentación y Registro	Revisión de la documentación asociada al Sistema de Gestión de Seguridad de la Información (Manual Políticas, Resolución, lineamientos, etc.) e identificación de necesidades de actualización	01/05/2026	31/12/2026
	Implementar indicadores de seguridad y medición del desempeño del SGSI	01/03/2026	31/12/2026

8.2.1. Gestión de Capacitación y Sensibilización en Seguridad de la Información

Como parte de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y en articulación con el Modelo Integrado de Planeación y Gestión (MIPG), la entidad desarrolla actividades de capacitación y sensibilización orientadas a fortalecer la cultura de seguridad y privacidad de la información en funcionarios, contratistas y terceros.

Estas actividades se planifican, ejecutan y realizan seguimiento mediante el anexo **Plan de Cambio, Cultura, Apropiación, Capacitación y Sensibilización de Seguridad y Privacidad de la Información y Seguridad Digital**, el cual se articula con el presente Plan y hace parte integral del mismo como Anexo, orientando la gestión del cambio y la apropiación de prácticas de seguridad y privacidad de la información en la entidad.

8.2.2. Gestión de Comunicaciones en Seguridad de la Información

Con el fin de asegurar la divulgación, apropiación y sostenibilidad del Modelo de Seguridad y Privacidad de la Información (MSPI), la entidad define y ejecuta acciones de comunicación interna orientadas a promover buenas prácticas y el cumplimiento de los lineamientos en materia de seguridad y privacidad de la información.

Las estrategias y acciones de comunicación se encuentran definidas en el anexo **Plan de Comunicaciones del Modelo de Seguridad y Privacidad de la Información – MSPI**, el cual se articula con el presente Plan y hace parte integral del mismo como Anexo, orientando la gestión de las comunicaciones internas asociadas a la seguridad y privacidad de la información en la entidad.

8.2.3. Gestión de la Gobernanza del MSPI

Con el propósito de fortalecer la gobernanza y la toma de decisiones estratégicas del MSPI, se proyecta la participación activa y la presentación periódica de los temas relacionados con la seguridad y la privacidad de la información ante el Comité Institucional de Gestión y Desempeño (CIGD) y el Comité Institucional de Coordinación y Control Interno (CICCI).

Esta participación permite articular de manera efectiva la gestión de riesgos de seguridad de la información con el Modelo Integrado de Planeación y Gestión (MIPG), fortalecer el cumplimiento del marco normativo vigente y apoyar la toma de decisiones informadas por parte de la alta dirección. Como resultado, se contribuye a garantizar la integridad, confidencialidad y disponibilidad de los activos de información de la entidad.

Las actividades asociadas a este proceso se gestionan y documentan a través del anexo **Plan de Participación y Presentación en Temas de Seguridad y Privacidad de la Información ante el CIGD y el CICCI**

HISTORIAL DE CAMBIOS

Versión	Descripción	Fecha
1	Primera Versión del Documento.	29/01/2020
2	Segunda versión del documento. Se actualiza versión por cambios organizacionales y normativos, entre otros, la transición de la política de Gobierno En Línea por la Política de Gobierno Digital	29/01/2021
3	Tercera versión del documento	15/01/2022
4	Cuarta versión del documento. Se elabora este documento como parte de la implementación de la gestión de riesgos de seguridad digital para asegurar la confidencialidad, integridad y disponibilidad de los activos de información	23/01/2023
5	Quinta versión del documento. Se realiza actualización y creación de nuevos apartes del presente documento como parte de la implementación de la gestión de riesgos de seguridad digital con el fin de articular las capacidades institucionales en el aseguramiento de la confidencialidad, integridad y disponibilidad de los activos de información	17/01/2024
6	Sexta versión: Se realiza actualización y creación de nuevos apartes del presente documento como parte de la implementación de la identificación y gestión de riesgos de seguridad de la información con el fin de articular las capacidades institucionales en el aseguramiento de la confidencialidad, integridad y disponibilidad de los activos de información.	23/01/2025
7	Séptima versión: se actualiza versión conforme a lo dispuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC en el Modelo de Seguridad y Privacidad de la Información (MSPI) 2025, expedido el 3 de junio de 2025, incluyendo ajustes en la gestión de riesgos y el fortalecimiento de los controles orientados a la protección de los activos de información. Se incluyen los siguientes anexos: • Plan de Cambio, Cultura, Apropiación, Capacitación y Sensibilización de Seguridad y Privacidad de la Información y Seguridad Digital • Plan de Comunicaciones del Modelo de Seguridad y Privacidad de la Información – MSPI • Plan de Participación y Presentación en Temas de Seguridad y Privacidad de la Información ante el CIGD y el CICCI	27/01/2026

APROBACIÓN				
	NOMBRE	**CARGO**	**FIRMA**	**FECHA**
ELABORÓ	Andrea Linney Sierra Ladino	Contratista - Subdirección Sistema Información de Tierras	**ORIGINAL FIRMADO**	21/01/2026
ELABORÓ	Rosa Johanna Rincón Molina	Contratista - Subdirección Sistema Información de Tierras	**ORIGINAL FIRMADO**	21/01/2026
ELABORÓ	Dianalin Neme Prada	Contratista - Subdirección Sistema Información de Tierras	**ORIGINAL FIRMADO**	21/01/2026
ELABORÓ	Guillermo Alfonso Ibagué Pinilla	Contratista - Subdirección Sistema Información de Tierras	**ORIGINAL FIRMADO**	21/01/2026
REVISÓ	Diana Lucía Herrera Riaño	Subdirectora de Sistemas de Información de Tierras	**ORIGINAL FIRMADO**	23/01/2026
APROBÓ	**APROBACIÓN Y PUBLICACIÓN DE LA POLÍTICA 1er Sesión Comité Institucional de Gestión y Desempeño del 27/01/2026**			

ANEXO
PLAN DE CAMBIO, CULTURA, APROPIACIÓN, CAPACITACIÓN Y SENSIBILIZACIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL.

1. Objetivo

Desarrollar competencias y fortalecer la conciencia en seguridad de la información en los funcionarios, contratistas y proveedores de la Agencia Nacional de Tierras, de acuerdo con sus roles y responsabilidades, con el fin de reducir los riesgos asociados al factor humano, apoyar la apropiación del MSPI y contribuir a la protección de los activos de información, en coherencia con la capacidad operativa institucional y los marcos normativos aplicables.

2. Alcance

El presente plan aplica para funcionarios, contratistas, proveedores y terceros que tengan acceso a la información o a los sistemas de la Agencia Nacional de Tierras, incluyendo directivos, líderes de proceso y personal técnico. Contempla actividades de inducción, capacitación periódica y refuerzo, de acuerdo con el rol y nivel de acceso de cada participante.

3. Marco Normativo de Referencia

- ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información
- NIST Cybersecurity Framework 2.0
- Modelo de Seguridad y Privacidad de la Información MINTIC – MSPI (2025)
- Ley 1581 de 2012 – Protección de Datos Personales
- CONPES 4144 de 2025 – Política Nacional de Inteligencia Artificial
- CONPES 3995 de 2020 – Confianza y Seguridad Digital
- CONPES 3854 de 2017 – Política Nacional de Seguridad Digital
- CONPES 3701 de 2011 – Lineamientos de Ciberseguridad y Ciberdefensa

4. Enfoque basado en roles y clasificación del público objetivo

Este plan se estructura bajo un enfoque basado en roles y nivel de riesgo, teniendo en cuenta las responsabilidades frente a la información, el nivel de acceso a los activos de información, el impacto potencial ante incidentes de seguridad y la relación contractual o funcional con la Entidad.

Con base en este enfoque, se definen los siguientes grupos de capacitación, lo que permite priorizar contenidos, optimizar recursos y asegurar una cobertura efectiva del personal interno y de terceros:

- Alta Dirección y directivos
- Líderes de proceso
- Personal técnico, de TI, Equipo de seguridad
- Funcionarios y contratistas

- Proveedores y terceros

5. Temáticas de capacitación diferenciadas por tipo de rol

Rol	Enfoque de la capacitación	Temáticas de capacitación
Alta Dirección	Gobernanza, toma de decisiones y gestión del riesgo, protección de datos personales. Cultura de Seguridad.	Lineamientos del MSPI y del SGSI; Sistema de Gestión de Continuidad del Negocio (SGCN); Tratamiento de Datos Personales (TDP); gobernanza y gestión de riesgos de seguridad de la información; fundamentos de ciberseguridad; riesgos tecnológicos relevantes, incluido el uso de Inteligencia Artificial. Responsabilidad del responsable del Tratamiento, sanciones, reputación. Liderazgo y ejemplo organizacional.
Líderes de proceso	Gestión del riesgo operativo y responsabilidades del proceso. Cultura de Seguridad. Derechos de Autor	Lineamientos del MSPI y del SGSI; Sistema de Gestión de Continuidad del Negocio (SGCN); Tratamiento de Datos Personales (TDP); gestión de riesgos del proceso; controles de seguridad aplicables; fundamentos de ciberseguridad; uso seguro de herramientas tecnológicas, incluida la Inteligencia Artificial. Liderazgo y ejemplo organizacional. Riesgos legales por uso indebido de software y contenidos
Personal técnico / TI / Seguridad de la Información	Implementación, operación y mejora de los controles de seguridad. Derechos de Autor	MSPI y SGSI; Sistema de Gestión de Continuidad del Negocio (SGCN); Tratamiento de Datos Personales (TDP); implementación y operación de controles de seguridad (Controles organizacionales, personas, físicos y tecnológicos); marco NIST CSF 2.0; gestión de riesgos de ciberseguridad; monitoreo y gestión de incidentes; ejercicios y pruebas; auditoría y mejora continua; gestión de riesgos asociados al uso de tecnologías emergentes, incluida la Inteligencia Artificial. Riesgos legales por uso indebido de software y contenidos
Funcionarios	Concienciación y reducción del riesgo humano Sensibilización en Seguridad y protección de la Información Derechos de Autor Manejo Seguro de la Información	Fundamentos del MSPI y del SGSI; Tratamiento de Datos Personales (TDP); uso seguro de la información y controles básicos; fundamentos de ciberseguridad; concienciación sobre riesgos asociados al uso de herramientas tecnológicas, incluida la Inteligencia Artificial. Qué es la información, por qué protegerla, clasificación. Principios, derechos del titular, deberes del funcionario y contratista.
Contratistas / usuarios finales	Concienciación y reducción del riesgo humano Sensibilización en Seguridad y protección de la Información Derechos de Autor	Fundamentos del MSPI y del SGSI; Tratamiento de Datos Personales (TDP); uso seguro de la información y controles básicos; fundamentos de ciberseguridad; concienciación sobre riesgos asociados al uso de herramientas tecnológicas, incluida la Inteligencia Artificial. Qué es la información, por qué protegerla, clasificación. Principios, derechos del titular, deberes del funcionario y contratista.

Rol	Enfoque de la capacitación	Temáticas de capacitación
	Manejo Seguro de la Información	
Proveedores y terceros	Cumplimiento y gestión del riesgo de terceros	Responsabilidades contractuales en seguridad y privacidad de la información; lineamientos mínimos para el manejo seguro de la información compartida; reporte de incidentes de seguridad.

Las temáticas se definen con base en el rol, nivel de responsabilidad y exposición al riesgo, conforme al enfoque de concienciación exigido por ISO/IEC 27001:2022 y el MSPI.

6. Modalidades de capacitación y sensibilización

Con el fin de garantizar la viabilidad operativa, se priorizan:

- Cursos virtuales
- Inducción y reinducción
- Microlearning
- Talleres focalizados
- Simulaciones específicas
- Piezas gráficas informativas

7. Articulación con el Plan de Comunicaciones del MSPI

Las capacitaciones se apoyan en las estrategias definidas en el Plan de Comunicaciones del Modelo de Seguridad y Privacidad De La Información - MSPI, utilizando los canales institucionales para:

- Convocatoria a capacitaciones
- Refuerzo de mensajes clave
- Divulgación de buenas prácticas
- Sensibilización continua

8. Indicadores de seguimiento

La medición y el seguimiento del plan se realizan bajo un enfoque diferenciado por tipo de rol, con priorización basada en el nivel de riesgo y mediante muestras representativas, en concordancia con la capacidad operativa de la entidad:

- Porcentaje de personal capacitado por rol.
- Resultados de evaluaciones de conocimiento.
- Resultados de simulaciones (cuando aplique).

- Número de capacitaciones ejecutadas frente a las programadas.

9. Evidencias

Las evidencias del este plan respaldan la ejecución de las actividades de difusión, capacitación y concientización en seguridad de la información dirigidas a funcionarios, contratistas y terceros, y permiten demostrar su realización periódica y su aporte a la reducción de riesgos asociados al factor humano:

- Registros de asistencia
- Certificados o constancias de capacitación
- Resultados de evaluaciones
- Informes de simulacros
- Material de capacitación utilizado
- Piezas graficas de las campañas

10. Responsables

- **Alta Dirección**: Apoyo y liderazgo en la implementación y cumplimiento del Plan.
- **Oficial de Seguridad de la Información:** Coordinación general del plan.
- **Equipo de Seguridad de la Información:** definición de contenidos, priorización y seguimiento del plan.
- **Subdirección de Talento Humano:** apoyo en la gestión y registro de capacitaciones.
- **Oficina de Comunicaciones:** apoyo en divulgación y sensibilización.
- **Líderes de proceso y supervisores de contrato:** gestión, promoción y seguimiento de la participación de sus equipos en las actividades de capacitación.
- **Subdirección Administrativa y Financiera**: Apoyo con la coordinación y asignación de recursos necesarios.

11. Actualización y aprobación del Plan

El Plan de Capacitaciones será revisado y actualizado anualmente o cuando se presenten cambios relevantes en el MSPI, el contexto de riesgo, la normativa aplicable o la estructura organizacional de la entidad, el mismo se aprueba como anexo al Plan de Seguridad y Privacidad de la Información.

ANEXO
PLAN DE COMUNICACIONES DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI

1. Objetivo

Definir y ejecutar las estrategias de comunicación para la gestión del cambio, la sensibilización y la apropiación de la Seguridad y Privacidad de la Información, dirigidas a funcionarios, contratistas y partes interesadas externas de la Agencia Nacional de Tierras, estableciendo los medios, mensajes y responsables que permitan difundir y fortalecer la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), promoviendo una cultura organizacional orientada a la protección de la información.

2. Alcance

Este plan aplica a todos los funcionarios, contratistas y partes interesadas de la Entidad, y abarca los canales internos de comunicación, actividades de sensibilización y divulgación asociadas al MSPI.

3. Públicos Objetivo

Público Objetivo	Características	Necesidades de información
Funcionarios de planta	Personal administrativo y operativo	Conocer roles, buenas prácticas, políticas y procedimientos del MSPI
Contratistas	Apoyo a procesos institucionales y misionales	Conocer roles, buenas prácticas, políticas y procedimientos del MSPI
Directivos y líderes	Toma de decisiones	Información estratégica y cumplimiento de responsabilidades
Partes interesadas externas	Proveedores, aliados, ciudadanía (si aplica)	Lineamientos sobre manejo seguro de la información compartida
Personal técnico / TI / Seguridad de la Información	Implementación, operación y mejora de los controles de seguridad. Derechos de Autor	Conocer comunicaciones especificas técnicas sobre amenazas, vulnerabilidades, alertas u otros.

4. Estrategias de Comunicación

- Diseño y difusión de infografías sobre principios del MSPI.
- Boletines electrónicos con tips de seguridad digital.
- Campañas de correo electrónico temáticas.
- Videos cortos o animaciones sobre prácticas seguras.
- Inclusión de mensajes en la Intranet.
- Podcast u otros medios.

5. Canales de Comunicación

Canal	Tipo	Uso previsto
Correo institucional	Digital	Difusión de campañas, infografías y alertas
Intranet	Digital	Publicación de recursos, manuales y políticas
Reuniones	Presencial / virtual	Sensibilización
Carteleras virtuales	Visual	Mensajes visuales de recordación y notificación
Fondos de escritorio y pantallas de bloqueo en los PC	Digital	Difusión de campañas, infografías y alertas

6. Cronograma de Actividades

El detalle de las actividades se puede consultar en el archivo: Plan de cambio, cultura, apropiación, capacitación y sensibilización de Seguridad y Privacidad de la Información y seguridad digital.xlsx

7. Indicadores de Seguimiento

Nº	Indicador	Fórmula	Frecuencia	Fuente de información	Meta sugerida
1	**Porcentaje de comunicaciones ejecutadas**	(Comunicaciones realizadas / Comunicaciones planificadas del periodo) × 100	Semestral	Plan de comunicaciones MSPI	≥ 90 %
2	**Porcentaje de población vigente que reciben comunicaciones**	(Destinatarios de la comunicación / Total de	Semestral	Listas de correo / Talento Humano / Contratación	≥ 50 %

Nº	Indicador	Fórmula	Frecuencia	Fuente de información	Meta sugerida
		personas vigentes en el periodo) × 100			
3	**Número de campañas de sensibilización realizadas sobre MSPI, SGSI, Ciberseguridad, IA, Derechos de autor, Tratamiento de datos personales entre otros.**	Conteo de campañas ejecutadas	Anual	Evidencias (correos, piezas gráficas, intranet)	≥ 4 campañas

8. Responsables del Plan

- **Alta Dirección**: Apoyo y liderazgo en la implementación y cumplimiento del Plan.
- **Oficial de Seguridad de la Información:** Coordinación general del plan.
- **Equipo de Seguridad de la Información:** definición de contenidos, priorización y seguimiento del plan.
- **Subdirección de Talento Humano:** apoyo en la gestión y registro de comunicaciones.
- **Oficina de Comunicaciones:** apoyo en divulgación y sensibilización.
- **Líderes de proceso y supervisores de contrato:** gestión, promoción y seguimiento de la participación de sus equipos en las actividades de comunicación.
- **Subdirección Administrativa y Financiera**: Apoyo con la coordinación y asignación de recursos necesarios.

9. Actualización del Plan

Este plan será revisado y actualizado anualmente o cuando se presenten cambios relevantes en el MSPI, el contexto de riesgo, la normativa aplicable o la estructura organizacional de la entidad, el mismo se aprueba como anexo al Plan de Seguridad y Privacidad de la Información.

ANEXO
PLAN DE PARTICIPACIÓN Y PRESENTACIÓN DE TEMAS EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ANTE EL CIGD Y EL CICCI

1. Objetivo

Definir la participación de la Subdirección de Sistemas de Información de Tierras en las sesiones del Comité Institucional de Gestión y Desempeño (**CIGD**) y del Comité Institucional de Coordinación y Control Interno (**CICCI**), mediante la presentación y el seguimiento de los temas, documentos y resultados en materia de seguridad y privacidad de la información que, por disposiciones de gubernamentales y normativas vigentes, deben ser puestos a consideración de estas instancias.

2. Alcance

El presente plan aplica a la preparación, presentación y seguimiento de los temas y documentos de seguridad y privacidad de la información gestionados por la Subdirección de Sistemas de Información de Tierras, en el marco de las sesiones del CIGD y del CICCI programadas por dichas instancias, durante la vigencia correspondiente.

3. Responsables

Responsable de preparación y presentación de temas en materia de Seguridad y Privacidad de la Información:

- Subdirección de Sistemas de Información de Tierras (SSIT)

Instancias responsables de la convocatoria, programación de sesiones y decisiones:

- Comité Institucional de Gestión y Desempeño (CIGD)
- Comité Institucional de Coordinación y Control Interno (CICCI)

4. Temas y documentos a presentar

En el marco de las disposiciones gubernamentales y normativas vigentes, y conforme al Modelo de Seguridad y Privacidad de la Información (MSPI), la Subdirección de Sistemas de Información presentará ante el CIGD y el CICCI los siguientes temas, documentos y resultados, como evidencia de la gestión realizada a través del Sistema de Gestión de Seguridad de la Información (SGSI)

Plan de Seguridad y Privacidad de la Información.

- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Políticas y lineamientos de seguridad y privacidad de la información (cuando se requiera adopción o actualización).
- Mapa de Riesgos de Seguridad de la Información.
- Inventario de Activos de Información.
- Continuidad del Negocio (BIA, BCP y DRP).

- Avances y resultados de la gestión de seguridad y privacidad de la información, como evidencia del funcionamiento del SGSI, en el marco del MSPI.

5. Participación y presentación ante el CIGD

La participación de la Subdirección de Sistemas de Información de Tierras en el CIGD se realizará en las sesiones convocadas por la Secretaría Técnica del Comité, conforme a la periodicidad establecida.

Trimestre	Tema	Gestión
Trimestre 1	Plan de Seguridad y Privacidad de la Información	Aprobación
	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Aprobación
	Políticas y lineamientos de seguridad y privacidad de la información (cuando aplique)	Aprobación
Trimestre 2	Estado del Modelo de Seguridad y Privacidad de la Información - MSPI	Seguimiento
	Políticas y lineamientos de seguridad y privacidad de la información (cuando aplique)	Aprobación
	Avances de la gestión de Continuidad del Negocio	Seguimiento
Trimestre 3	Estado del Modelo de Seguridad y Privacidad de la Información - MSPI	Seguimiento
	Políticas y lineamientos de seguridad y privacidad de la información (cuando aplique)	Seguimiento
Trimestre 4	Continuidad del Negocio (BIA, BCP y DRP)	Aprobación
	Mapa de Riesgos de Seguridad de la Información	Aprobación
	Inventario de Activos de Información	Aprobación
	Autodiagnóstico del Modelo de Seguridad y Privacidad de la Información - MSPI	Aprobación
	Políticas y lineamientos de seguridad y privacidad de la información (cuando aplique)	Aprobación

6. Participación y presentación ante el CICCI

La Subdirección de Sistemas de Información de Tierras participará en las sesiones del CICCI para la presentación de los temas relacionados con los riesgos de seguridad y privacidad de la información, de acuerdo con la agenda definida por dicho comité.

7. Seguimiento

La Subdirección de Sistemas de Información de Tierras realizará el seguimiento a las decisiones, observaciones y aprobaciones emitidas por el CIGD y el CICCI, incorporando los ajustes requeridos en los documentos y asegurando la trazabilidad correspondiente en las actas y soportes institucionales.

8. Resultado esperado

- Participación efectiva de la Subdirección de Sistemas de Información de Tierras en los comités institucionales.
- Presentación oportuna de los temas y documentos obligatorios en materia de seguridad y privacidad de la información.
- Fortalecimiento de la toma de decisiones en materia de seguridad y privacidad de la información.
- Cumplimiento de las disposiciones normativas aplicables.