Plan de Seguridad y Privacidad de la Información

Ministerio de las Culturas, las Artes y los Saberes.

2026

"Se consideran copias controladas los documentos que se encuentran vigentes en ISOLUCIÓN"

Contenido

1. INTRODUCCIÓN

En el marco de la evolución del gobierno electrónico en Colombia y en consonancia con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG), la política de gobierno digital y el modelo de seguridad y privacidad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Ministerio de las Culturas, las Artes y los Saberes adapta su estrategia institucional.

La Política de Gobierno Digital del Estado Colombiano establece una gobernanza que fomenta la interacción entre los niveles nacional y territorial, así como entre el central y el descentralizado, involucrando a los grupos de interés relevantes. Esta política se articula en torno a cuatro habilitadores claves: arquitectura empresarial, seguridad y privacidad de la información, cultura y apropiación, y servicios ciudadanos digitales. Estos habilitadores son esenciales para implementar las líneas de acción definidas y las iniciativas dinamizadoras propuestas.

En el Ministerio de las Culturas, las Artes y los Saberes, la seguridad y privacidad de la información se ha identificado como un habilitador importante, en línea con lo establecido en la Resolución 500 de 2021 del MinTIC, que dicta los lineamientos y estándares para la estrategia de seguridad digital. Conforme a esto, el Ministerio ha desarrollado un plan integral que fortalece los procesos, servicios e infraestructura de TI, asegurando la confidencialidad, integridad y disponibilidad de los activos de información. Esto es fundamental para apoyar la consecución de los objetivos institucionales y fortalecer la relación de confianza con todas las partes interesadas, resaltando el compromiso del Ministerio con la promoción y salvaguarda de la cultura, el arte y los saberes en el ámbito digital.

Este Plan de Seguridad y Privacidad de la Información para la vigencia 2026 se actualiza conforme a la Resolución 2277 de 2025 del Ministerio TIC, la cual actualiza el Anexo 1 de la Resolución 500 de 2021 (MSPI) y alinea el modelo con la norma ISO/IEC 27001:2022. En consecuencia, las actividades y líneas de acción aquí definidas se orientan al ciclo PHVA, la gestión de riesgos, la implementación de controles, la medición del desempeño y la mejora continua, integrando consideraciones de seguridad digital para proteger los activos de información y garantizar la continuidad de los servicios.

2. OBJETIVO

Establecer acciones específicas para fortalecer el Modelo de Seguridad y Privacidad de la Información en la entidad con el fin de asegurar la integridad, confidencialidad y disponibilidad de los activos de información institucionales.

OBJETIVOS ESPECÍFICOS

- Desarrollar un plan de acción específico para el año 2026, que incluya actividades destinadas a abordar y resolver las brechas identificadas en el MSPI.
- Determinar y asignar los recursos necesarios (humanos, financieros, tecnológicos) para la implementación eficiente del plan de seguridad y privacidad de la información.
- Fomentar una cultura organizacional de seguridad y privacidad de la información.
- Fortalecer la Seguridad Cibernética de los Recursos Tecnológicos

3. ALCANCE

El Plan de Seguridad de la Información del Ministerio de las Culturas, las

Artes y los Saberes, que complementa y robustece los lineamientos de la Política de Seguridad de la Información, es integral y aplica a todos los procesos y procedimientos del Ministerio, resaltando su importancia estratégica.

Este Plan cubre a todos los usuarios relacionados con el Ministerio, Incluyendo servidores públicos, personal de planta (permanente y temporal), contratistas, consultores, pasantes y proveedores involucrados en sus operaciones.

4. CONTEXTO INSTITUCIONAL

El alcance del presente documento aplica para el periodo comprendido en la vigencia 2026, para el Ministerio, entidad de orden nacional. Las actualizaciones que sean necesarias se surtirán adicionales a las previstas por anualidad. Si bien las iniciativas que resulten iniciando la vigencia 2026, podrán ser modificadas en contenido o cantidad de acuerdo con las novedades normativas o estratégicas de la entidad y del sector.

EL Plan Estratégico de Tecnologías de la Información PETI, inicia desde el entendimiento estratégico del Ministerio, análisis de la situación actual, contempla identificación de las necesidades de TI de la entidad, la definición de la estrategia de TI y finaliza con la definición del portafolio de iniciativas y la ruta que permitirán la ejecución de esta.

El Ministerio de las Culturas, las Artes y los Saberes, es el organismo rector de la cultura, encargado de formular, coordinar, ejecutar y vigilar la política del Estado en la materia, en concordancia con los planes y programas de desarrollo, según los principios de participación contemplados en esta ley; el Ministerio de las Culturas, las Artes y los Saberes tendrá a su cargo, además de las funciones previstas en la presente ley, el ejercicio de las atribuciones generales que corresponde ejercer a los ministerios, de conformidad con el Decreto 1050 de 1968.

Al Ministerio de las Culturas, las Artes y los Saberes, le corresponde liderar el proceso de coordinación intersectorial para fortalecer las instituciones públicas, privadas y mixtas, orientadas a la promoción, defensa, divulgación y desarrollo de las actividades culturales y creativas y promover adecuadamente el potencial de la economía cultural y creativa.

MISIÓN

Formular, coordinar e implementar la política del Estado para promover las condiciones que permitan el ejercicio de los derechos culturales en corresponsabilidad con los actores sociales e institucionales, para el fomento, protección y salvaguardia de las memorias, patrimonios, saberes, identidades y prácticas artísticas y culturales, como fundamento de la diversidad de la nación, la transformación social de los territorios y la construcción de una cultura de paz.

VISIÓN

En el 2038 el Ministerio de las Culturas, las Artes y los Saberes será líder en el fomento de las políticas para el ejercicio de los derechos culturales y la promoción de la cultura como bien público y de interés colectivo que contribuye al reconocimiento y protección de la diferencia y la diversidad, la transformación social, el diálogo intercultural y a la construcción de sociedades en paz.

CONTEXTO ESTRATÉGICO

El plan enmarcado en este documento contribuye al cumplimiento de los objetivos estratégicos, los cuales se encuentran establecidos en el Plan Estratégico Institucional -PEI.

CONTEXTO ESTRATEGICO ARTICULADO	
Objetivo Estratégico al que Contribuye	8.Fortalecer la capacidad de gestión y desempeño institucional y la mejora continua de los procesos, basada en la gestión de los riesgos, el manejo de la información y la evaluación para la toma de decisiones
Modelo Integrado de Planeación y Gestión - MIPG	Política Gobierno Digital Política de Seguridad Digital Política de Gestión Documental Política de Transparencia, acceso a la información pública y lucha contra la corrupción

Tabla 1: *Contexto Estratégico, Fuente: Plan Estratégico Ministerio de las Culturas, las Artes y los Saberes.*

5. REFERENCIAS

Normativa	Entidad	Descripción
Resolución 2277 de 2025	Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC	Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.
Circular Externa No. 002 del 21 de agosto de 2024	Superintendencia de Industria y Comercio	Lineamientos sobre el tratamiento de datos personales en sistemas de inteligencia artificial.
Resolución 460 de 2022	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno digital, y se dictan los

Normativa	Entidad	Descripción
		lineamientos generales para su implementación.
Resolución 500 de 2021	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
Decreto 620 de 2020	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Resolución 1519 de 2020.	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	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
Directiva 002 de 2020	Presidencia de la Republica	Medidas para atender la contingencia generada por el covid-19, a partir uso de las tecnologías la información y las telecomunicaciones - TIC
CONPES 3995 de 2020.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política Nacional de Confianza y Seguridad Digital.
Decreto 612 de 2018	Presidencia de la Republica	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

6. OPERACIÓN DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD

DE LA INFORMACIÓN - SGSI

CICLO DE OPERACIÓN

De acuerdo con el contexto particular del Ministerio de las Culturas, las Artes y los Saberes, y siguiendo la metodología del Modelo de Seguridad y Privacidad de la Información (MSPI), se implementa el Subsistema de Gestión de Seguridad de la Información y Seguridad Digital. Este subsistema opera basándose en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), incluyendo los requerimientos técnicos, normativos, reglamentarios y de funcionamiento específicos del Ministerio.

El modelo se estructura en cinco fases que facilitan la gestión eficaz y el mantenimiento de la seguridad y privacidad de los activos de información en el ámbito institucional.

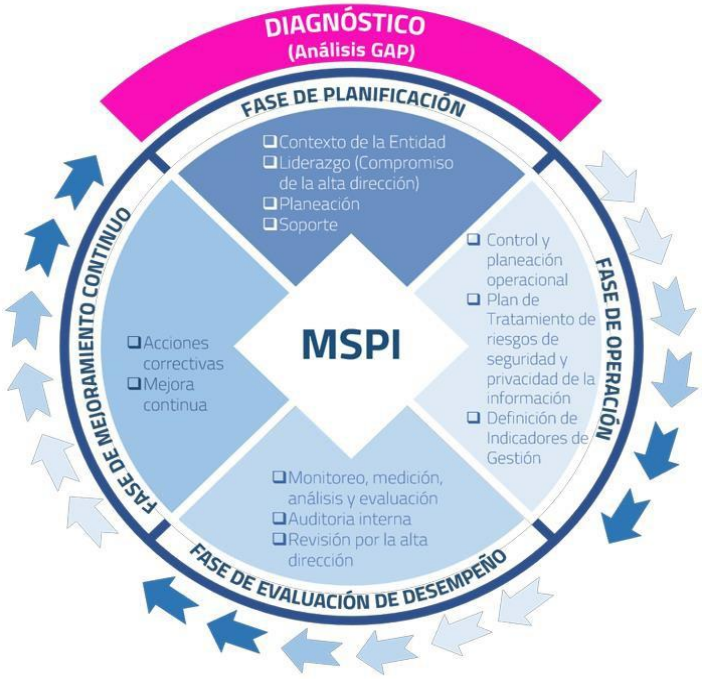

Ilustración 1. *Ciclo de operación del modelo de seguridad y privacidad de la información, Fuente: MinTic.*

DIAGNÓSTICO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI

En cumplimiento del ciclo de operación del Modelo de Seguridad y Privacidad de la Información (MSPI) y conforme a los lineamientos del Ministerio TIC, durante la vigencia 2025 el Ministerio de las Culturas, las Artes y los Saberes realizó el autodiagnóstico institucional del MSPI, alineado con la norma ISO/IEC 27001:2022.

El resultado del autodiagnóstico evidencia un nivel general de madurez optimizado, con un promedio global del 87%, distribuidos de la siguiente manera:

- Dominio Organizacional: 85%
- Dominio Personas: 90%
- Dominio Físico: 89%
- Dominio Tecnológico: 82%
- Marco NIST: 90,03%

El presente Plan de Seguridad y Privacidad de la Información 2026 se formula como respuesta directa a las brechas identificadas, permitiendo cerrar el ciclo PHVA mediante acciones planificadas y orientadas a la mejora continua del SGSI.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	85	100	OPTIMIZADO
A.6	CONTROLES DE PERSONAS	90	100	OPTIMIZADO
A.7	CONTROLES FÍSICOS	89	100	OPTIMIZADO
A.8	CONTROLES TECNOLÓGICOS	82	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		87	100	OPTIMIZADO

Ilustración 2. *Portada, documento Autodiagnostico_MSPI_MINCULTURAS_2025*

7. ESTRATEGIAS

Las actividades aquí establecidas se estructuran bajo un enfoque operativo, medible y basado en riesgos, incorporando responsables, productos, tiempos de ejecución y resultados esperados, lo que permite su trazabilidad, seguimiento y evaluación del desempeño. Estas acciones se derivan del autodiagnóstico institucional del MSPI, de las brechas identificadas en los dominios organizacional, personas, físico y tecnológico, y de los eventos relevantes ocurridos en vigencias anteriores.

Las estrategias se organizan en cuatro componentes que articulan el ciclo de gestión del SGSI:

- Planificación: orientada a la identificación de brechas, gestión de activos, riesgos y fortalecimiento de capacidades.
- Operación: enfocada en la implementación de controles, políticas, mecanismos técnicos, gestión de incidentes y continuidad.
- Evaluación de Desempeño: destinada a medir la eficacia del plan, el cumplimiento de los controles y el avance de la hoja de ruta.
- Mejora Continua: orientada a la corrección de brechas, fortalecimiento de controles y adaptación a cambios normativos, tecnológicos y organizacionales.

Planificación

Autodiagnóstico

Eje	Gobierno y Gestión de la Seguridad de la Información
Actividad	Actualizar el instrumento de autodiagnóstico institucional del MSPI conforme a la Resolución 2277 de 2025, recopilando evidencias de los dominios organizacional, personas, físico y tecnológico.
Producto	Informe de Autodiagnóstico MSPI 2026 con análisis de brechas, nivel de madurez por dominio y plan preliminar de mejora.
Tiempo estimado	2 meses (Junio – julio 2026)
Responsable	Oficial de Seguridad de la Información, con apoyo del Grupo de Infraestructura y sistemas de Información de la OTI

Gestión de activos de información

Eje	Gestión de Activos de Información
Actividad	Ejecutar el procedimiento institucional para la identificación, clasificación, actualización, protección y publicación controlada de los activos de información, mediante acciones de sensibilización, solicitud formal a los líderes de proceso, validación técnica, consolidación de la matriz institucional, anonimización de la información clasificada y reservada, y gestión de su publicación, garantizando el cumplimiento de los principios de transparencia, confidencialidad, integridad y disponibilidad. Actividades específicas: ◆ Charla de sensibilización sobre activos de información ◆ Revisión y retroalimentación ◆ Consolidación de matriz institucional ◆ Anonimización y generación del índice ◆ Publicación en datos abiertos
Producto	Matriz institucional de activos de información actualizada, clasificada y publicada (cuando aplique), con soporte de sensibilización, validación y control de acceso.
Tiempo estimado	5 meses (julio – noviembre 2026).
Responsable	Líderes de proceso, con apoyo del Oficial de Seguridad de la Información

Gestión de riesgos de seguridad de la información

Eje	Gestión de Riesgos de Seguridad de la Información
Actividad	Identificar, analizar, evaluar y priorizar los riesgos de seguridad de la información asociados a los activos institucionales con nivel de criticidad alto, mediante la aplicación de la metodología institucional de gestión del riesgo, con el fin de definir acciones de tratamiento que mitiguen los impactos sobre la

Eje	Gestión de Riesgos de Seguridad de la Información
	confidencialidad, integridad y disponibilidad de la información y soporten la toma de decisiones. **Actividades específicas:** ◆ Identificación de activos críticos y sus amenazas asociadas ◆ Análisis y valoración de riesgos (probabilidad e impacto) ◆ Priorización de riesgos y definición de criterios de aceptación ◆ Formulación del Plan de Tratamiento de Riesgos ◆ Socialización y validación con los líderes de proceso
Producto	Matriz institucional de riesgos de seguridad de la información y Plan de Tratamiento de Riesgos, documentados en ISOLUCION
Tiempo estimado	3 meses (marzo – mayo 2026)
Responsable	Todos los procesos, con apoyo del Oficial de Seguridad de la Información

Cultura y apropiación

Eje	Cultura y Apropiación en Seguridad de la Información
Actividad	Diseñar e implementar acciones de sensibilización, formación y evaluación orientadas a fortalecer la cultura organizacional en seguridad y privacidad de la información, promoviendo comportamientos seguros, el cumplimiento de los lineamientos institucionales y la apropiación de los procedimientos asociados al SGSI. **Actividades específicas:** ◆ Elaboración de la matriz de cultura y apropiación en seguridad de la información para la vigencia 2026 ◆ Ejecución de campañas de sensibilización y jornadas de formación dirigidas a servidores públicos y contratistas

Eje	Cultura y Apropiación en Seguridad de la Información
	◆ Diseño y ejecución de ejercicios controlados de phishing e ingeniería social ◆ Medición del nivel de apropiación mediante encuestas, simulaciones y análisis de resultados ◆ Socialización de resultados y definición de acciones de mejora
Producto	Reporte de simulación
Tiempo estimado	2 meses (abril – mayo 2026)
Responsable	Oficial de Seguridad de la Información, con apoyo de proveedor de ciberseguridad

Operación

Implementación

Eje	Gestión de Vulnerabilidades
Actividad	Definir, implementar y operar el proceso institucional de gestión de vulnerabilidades técnicas sobre la infraestructura y los sistemas de información, con el fin de identificar, evaluar, priorizar y tratar debilidades de seguridad que puedan ser explotadas. **Actividades específicas:** ◆ Actualización del procedimiento institucional de gestión de vulnerabilidades ◆ Definición del alcance y periodicidad de los análisis ◆ Ejecución de análisis técnicos (escaneo, validación y correlación) ◆ Clasificación de vulnerabilidades por criticidad ◆ Formulación y seguimiento del plan de remediación

Eje	Gestión de Vulnerabilidades
Producto	Procedimiento aprobado, informes de análisis, matriz de vulnerabilidades y sesiones de seguimiento sobre remediación
Tiempo estimado	Actividad permanente durante la vigencia 2026.
Responsable	Proveedor de ciberseguridad, Oficial de Seguridad de la Información, Grupo de Infraestructura y sistemas de Información del Ministerio, Biblioteca y Museo Nacional

Eje	Gobernanza y Protección de Datos
Actividad	Actualizar, armonizar y socializar las políticas institucionales de seguridad y protección de datos personales, garantizando su alineación con la Ley 1581 de 2012, la Resolución 2277 de 2025 y el MSPI. **Actividades específicas:** ◆ Actualización de la Política de Seguridad y Privacidad de la Información ◆ Actualización de la Política de Protección de Datos Personales ◆ Socialización institucional ◆ Actualización del RNBD
Producto	Políticas aprobadas, piezas gráficas, RNBD actualizado.
Tiempo estimado	6 meses (marzo – septiembre 2026).
Responsable	Oficial de Seguridad de la Información, líderes de proceso

Eje	Protección Tecnológica
Actividad	Implementar mecanismos técnicos de protección de la información y control de accesos, priorizando los activos críticos, garantizando confidencialidad, integridad y trazabilidad. **Actividades específicas:** ◆ Evaluación de cifrado en portátiles y bases de datos ◆ Implementación de cifrado cuando sea viable
Producto	Informe técnico, controles implementados
Tiempo estimado	6 meses (abril – septiembre 2026)
Responsable	Administrador base de datos, mesa de ayuda, Oficial de Seguridad de la Información

Eje	Gestión de accesos y control de privilegios
Actividad	Definir, implementar y mantener actualizada la matriz institucional de roles y perfiles de acceso para los sistemas de información, aplicando el principio de mínimo privilegio y estableciendo mecanismos de auditoría periódica, con el fin de garantizar la trazabilidad, la segregación de funciones y la prevención de accesos no autorizados a la información. **Actividades específicas:** ◆ Definición y documentación de la matriz de roles y perfiles de acceso por sistema de información ◆ Revisión y depuración de permisos existentes conforme al principio de mínimo privilegio
Producto	Matriz institucional de roles y perfiles, reportes/informes de acciones aplicadas
Tiempo estimado	5 meses (mayo – septiembre 2026).

Eje	Gestión de accesos y control de privilegios
Responsable	Todas las áreas que tienen a cargo desarrollos de sistemas de información, con apoyo de la coordinación de sistemas de información de la OTI

Gestión de incidentes de seguridad de la información

Eje	Gestión de Incidentes de Seguridad de la Información
Actividad	Operar y fortalecer el procedimiento institucional de gestión de incidentes de seguridad de la información, garantizando la detección, análisis, contención, erradicación, recuperación, comunicación y cierre de los incidentes, con el fin de minimizar su impacto sobre los servicios, los activos de información y la continuidad institucional. **Actividades específicas:** ◆ Socialización del procedimiento de gestión de incidentes ◆ Monitoreo permanente de eventos y alertas de seguridad
Producto	Piezas gráficas, correos electrónicos con gestión de alertas/eventos
Tiempo estimado	Actividad permanente durante la vigencia 2026.
Responsable	Oficial de Seguridad de la Información, Grupo de Infraestructura y sistemas de Información del Ministerio, Biblioteca y Museo Nacional

Gestión de la documentación del SGSI

Eje	Gestión de la Información Documentada del SGSI
Actividad	Revisar, actualizar y mantener controlada la documentación asociada al Sistema de Gestión de Seguridad de la Información, garantizando su vigencia, coherencia normativa y alineación con los procesos, controles y riesgos institucionales.

Eje	Gestión de la Información Documentada del SGSI
	Actividades específicas: ◆ Identificación y priorización de los documentos del SGSI a actualizar (políticas, procedimientos, guías, formatos y registros). ◆ Revisión de coherencia frente a MSPI, ISO/IEC 27001:2022 y normativa nacional aplicable. ◆ Actualización y control de versiones de la documentación. ◆ Aprobación y publicación institucional. ◆ Socialización de los cambios con los responsables de proceso.
Producto	Repositorio institucional (ISOLUCION) de documentos del SGSI actualizado, control de versiones
Tiempo estimado	Actividad permanente durante la vigencia 2026 (con revisión semestral).
Responsable	Oficial de Seguridad de la Información

Continuidad de seguridad de la información

Eje	Continuidad y Resiliencia de los Servicios de TI
Actividad	Implementar un enfoque progresivo de continuidad, mediante la identificación de un servicio crítico priorizado y la documentación de su Plan de Recuperación ante Desastres (DRP), complementado con pruebas de restauración y revisiones periódicas de las copias de seguridad, con el fin de fortalecer gradualmente la capacidad de respuesta ante eventos disruptivos. **Actividades específicas:** ◆ Identificar y priorizar un servicio crítico mediante criterios de impacto operativo, legal y reputacional. ◆ Documentar el DRP específico para el servicio priorizado.

Eje	Continuidad y Resiliencia de los Servicios de TI
	◆ Ejecutar y documentar restauraciones aleatorias sobre copias de seguridad. ◆ Ejecutar revisiones periódicas sobre la funcionalidad, errores y eventos de la solución de respaldo.
Producto	DRP documentado para un servicio crítico, informes de restauración, reportes de revisión de respaldos
Tiempo estimado	6 meses (julio – diciembre 2026).
Responsable	Oficina Tecnologías de la Información, con acompañamiento del Oficial de Seguridad de la Información.

Evaluación de Desempeño

Eje	
Actividad	Medir, analizar y evaluar periódicamente el desempeño del Plan de Seguridad y Privacidad de la Información, mediante reportes y mecanismos de seguimiento, con el fin de verificar el cumplimiento del avance de la hoja de ruta.
Producto	Informe o reportes sobre la ejecución de actividades del plan de seguridad y privacidad de la información
Tiempo estimado	Actividad permanente durante la vigencia 2026.
Responsable	Oficial de Seguridad de la Información

Mejora Continua

Eje	
Actividad	Documentar, priorizar e implementar acciones correctivas y de mejora derivadas de auditorías, revisiones internas, incidentes, evaluaciones de desempeño y cambios en el contexto

Eje	
	institucional, con el fin de fortalecer de manera continua el Sistema de Gestión de Seguridad de la Información.
Producto	Plan de acciones de mejora, registros de seguimiento y evidencias de cierre de brechas en ISOLUCION
Tiempo estimado	Actividad permanente durante la vigencia 2026.
Responsable	Oficial de Seguridad de la Información, con apoyo del Grupo de Infraestructura y sistemas de Información del Ministerio

8. DEFINICIONES

- **Autodiagnóstico MSPI:** Ejercicio de autoevaluación institucional que permite medir el nivel de madurez del Modelo de Seguridad y Privacidad de la Información, identificar brechas y definir acciones de mejora alineadas al ciclo PHVA.
- **Base de datos personales:** Conjunto organizado de datos personales que es objeto de tratamiento por parte de la Entidad, independientemente del medio en el que se almacene.
- **Cifrado:** Mecanismo de protección de la información que transforma los datos en un formato no legible para personas no autorizadas, con el fin de salvaguardar su confidencialidad.
- **Gestión de accesos:** Conjunto de actividades orientadas a controlar, administrar y supervisar los permisos de acceso a los sistemas de información, garantizando el principio de mínimo privilegio.
- **Ingeniería social:** Conjunto de técnicas utilizadas para manipular a las personas y obtener información o accesos no autorizados, evaluadas en la Entidad mediante simulaciones controladas como el phishing.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información y las Comunicaciones como habilitador de la Política de Gobierno Digital.
- **RNBD:** Registro Nacional de Bases de Datos administrado por la Superintendencia de Industria y Comercio, en el cual deben inscribirse las bases de datos que contengan información personal.