MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI

INSTITUTO DE VIVIENDA DE INTERÉS SOCIAL Y REFORMA URBANA DE BUCARAMANGA – INVISBU

Vigencia: 2026

1. Introducción

El Instituto de Vivienda de Interés Social y Reforma Urbana de Bucaramanga – INVISBU adopta e implementa el **Modelo de Seguridad y Privacidad de la Información – MSPI** como marco institucional para la gestión integral de la seguridad, privacidad y seguridad digital de la información, en concordancia con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, la Política de Gobierno Digital y el Modelo Integrado de Planeación y Gestión – MIPG.

El MSPI orienta la implementación progresiva de medidas administrativas, técnicas, organizacionales y operativas dirigidas a proteger los activos de información institucionales y preservar los principios de **confidencialidad, integridad, disponibilidad y privacidad de la información**, teniendo en cuenta los riesgos, necesidades, recursos, características y capacidades del INVISBU.

La implementación del modelo se desarrolla mediante un ciclo de gestión compuesto por las fases de **Diagnóstico, Planificación, Operación, Evaluación del desempeño y Mejoramiento continuo**, permitiendo fortalecer progresivamente las capacidades institucionales en materia de seguridad y privacidad de la información.

El **Plan de Seguridad y Privacidad de la Información – PSPI 2026** constituye uno de los principales instrumentos para la planificación y ejecución de las actividades del MSPI y se articula con la gestión institucional de riesgos, los activos de información, la gestión de incidentes, la continuidad de los servicios tecnológicos y los demás instrumentos institucionales relacionados.

2. Objetivo general

Implementar y mantener el Modelo de Seguridad y Privacidad de la Información – MSPI en el INVISBU, mediante la aplicación progresiva de lineamientos, políticas, procesos, controles y acciones orientadas a proteger los activos de información institucionales y gestionar los riesgos que puedan afectar su confidencialidad, integridad, disponibilidad y privacidad.

3. Objetivos específicos

- Establecer el marco institucional para la gestión de la seguridad y privacidad de la información.
- Identificar, inventariar, valorar y clasificar los activos de información del INVISBU.
- Identificar, analizar, valorar y tratar los riesgos de seguridad y privacidad de la información.
- Definir e implementar controles administrativos, técnicos y organizacionales de acuerdo con los riesgos identificados.
- Fortalecer la gestión de incidentes de seguridad de la información.
- Fortalecer la continuidad, disponibilidad y recuperación de la información y de los servicios tecnológicos.
- Gestionar los riesgos asociados a terceros y proveedores que tengan acceso a información o infraestructura institucional.

- Promover la cultura, sensibilización y apropiación de prácticas seguras por parte de funcionarios, contratistas y terceros.
- Establecer mecanismos de medición, seguimiento, evaluación y mejora continua del MSPI.
- Articular la seguridad y privacidad de la información con el MIPG, la Política de Gobierno Digital, el PETI y los demás instrumentos institucionales aplicables.

4. Alcance del MSPI

El Modelo de Seguridad y Privacidad de la Información aplica a todos los procesos del INVISBU y comprende la información institucional generada, recibida, procesada, almacenada, transmitida o custodiada por la entidad, independientemente de su medio o formato.

El alcance comprende, entre otros:

- Funcionarios y contratistas.
- Procesos misionales, estratégicos, administrativos y de evaluación.
- Sistemas de información institucionales.
- Bases de datos.
- Infraestructura tecnológica.
- Equipos de cómputo.
- Servicios de comunicaciones y conectividad.
- Correo electrónico institucional y servicios Microsoft 365.
- Portal web y servicios digitales institucionales.
- Información física y digital.
- Proveedores y terceros con acceso autorizado a información o recursos tecnológicos institucionales.
- Servicios tecnológicos administrados directamente por el INVISBU o suministrados por terceros.

La implementación del MSPI será gradual y estará determinada por la criticidad de los activos, los riesgos identificados, las obligaciones legales y regulatorias, la disponibilidad presupuestal y las capacidades institucionales.

5. Marco normativo y de referencia

La implementación del MSPI en el INVISBU se desarrolla considerando, entre otras, las siguientes disposiciones y referentes:

- Constitución Política de Colombia, artículo 15.
- Ley 594 de 2000 – Ley General de Archivos.
- Ley 1273 de 2009 – Protección de la información y de los datos.
- Ley 1581 de 2012 – Protección de Datos Personales.
- Ley 1712 de 2014 – Transparencia y Derecho de Acceso a la Información Pública.
- Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector TIC y sus modificaciones.
- Decreto 338 de 2022 – Gobernanza de la seguridad digital.
- Decreto 767 de 2022 – Política de Gobierno Digital.

- Resolución MinTIC 1519 de 2020 y sus anexos aplicables.
- Resolución MinTIC 500 de 2021.
- Resolución MinTIC 746 de 2022.
- Resolución MinTIC 2277 de 2025, mediante la cual se actualiza el Anexo 1 de la Resolución 500 de 2021.
- Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI vigente.
- Lineamientos e instrumentos complementarios expedidos por el Ministerio TIC.
- Modelo Integrado de Planeación y Gestión – MIPG.
- Política de Gobierno Digital.

6. Gobierno del Modelo de Seguridad y Privacidad de la Información

La seguridad y privacidad de la información constituye una responsabilidad institucional y requiere la participación coordinada de la Alta Dirección, la Oficina Asesora TIC, los líderes de proceso, la Oficina de Control Interno, funcionarios, contratistas y proveedores.

6.1 Alta Dirección

Corresponde a la Alta Dirección:

- Respaldar institucionalmente la implementación y mejora del MSPI.
- Orientar las decisiones estratégicas relacionadas con seguridad y privacidad de la información.
- Promover la disponibilidad de los recursos requeridos para su implementación.
- Conocer los resultados del seguimiento y evaluación del modelo.
- Impulsar la adopción de acciones de mejora cuando sean necesarias.

6.2 Comité Institucional de Gestión y Desempeño

El Comité Institucional de Gestión y Desempeño constituye la instancia institucional para la presentación, aprobación, seguimiento y toma de decisiones estratégicas relacionadas con la implementación del MSPI, de conformidad con sus competencias.

6.3 Oficina Asesora TIC

La Oficina Asesora TIC ejerce el liderazgo técnico de la implementación del MSPI y coordina las actividades relacionadas con seguridad tecnológica, controles de seguridad, gestión de riesgos tecnológicos, gestión de incidentes, continuidad tecnológica, copias de seguridad, gestión de accesos y seguimiento al Plan de Seguridad y Privacidad de la Información.

6.4 Líderes de proceso

Los líderes de proceso son responsables de identificar, clasificar, custodiar y proteger la información correspondiente a sus procesos y de participar en la identificación, valoración y tratamiento de los riesgos asociados.

6.5 Oficina de Control Interno

La Oficina de Control Interno realizará la evaluación independiente del estado de implementación y efectividad del MSPI, de conformidad con sus competencias y con el esquema institucional de control.

6.6 Funcionarios, contratistas y proveedores

Son responsables de cumplir las políticas, procedimientos y controles de seguridad y privacidad establecidos por el INVISBU, proteger adecuadamente la información a la cual tengan acceso y reportar oportunamente los eventos o incidentes de seguridad de la información identificados.

7. CICLO DE IMPLEMENTACIÓN DEL MSPI

7.1 Fase de Diagnóstico

El INVISBU realiza el diagnóstico del estado de implementación del Modelo de Seguridad y Privacidad de la Información mediante la herramienta de autodiagnóstico definida para este propósito.
Para la vigencia 2026, la entidad cuenta con la **Matriz de Autodiagnóstico MSPI – Base 2026**, mediante la cual se identificaron los niveles de madurez, brechas y oportunidades de mejora institucionales.

Los resultados evidencian avances diferenciados entre los componentes evaluados, con niveles de madurez ubicados entre **Inicial, Básico y Gestionado**.

Se identificaron como áreas que requieren fortalecimiento prioritario:

- Gestión de riesgos de seguridad y privacidad de la información.
- Cultura y sensibilización.
- Gestión de proveedores y terceros.
- Formalización de controles operativos.
- Seguimiento y medición de la efectividad de los controles.

Los resultados del diagnóstico constituyen la línea base para la planificación, operación, evaluación y mejoramiento continuo del MSPI.

Evidencia principal: Matriz de Autodiagnóstico MSPI – INVISBU Base 2026.

7.2 Fase de Planificación

La fase de planificación establece las condiciones, prioridades, responsabilidades, recursos y acciones necesarias para implementar el MSPI.

7.2.1 Contexto institucional

El INVISBU desarrolla sus funciones mediante procesos estratégicos, misionales, de apoyo y evaluación que dependen del tratamiento permanente de información física y digital.

La operación institucional requiere el uso de infraestructura tecnológica, sistemas de información propios y de terceros, correo electrónico institucional, servicios en nube, equipos de usuario final, redes de comunicaciones, servicios web y diferentes repositorios documentales.

La existencia de información relacionada con beneficiarios, funcionarios, contratistas, proveedores, procesos financieros, contractuales y administrativos hace necesario establecer medidas de protección acordes con la naturaleza y criticidad de cada activo.

La implementación del MSPI considera las capacidades tecnológicas, humanas, presupuestales y organizacionales existentes en la entidad y adopta un enfoque progresivo basado en riesgos.

7.2.2 Partes interesadas

Para efectos del MSPI se consideran partes interesadas, entre otras:

- Ciudadanía y beneficiarios de los programas institucionales.
- Funcionarios.
- Contratistas.
- Alta Dirección.
- Líderes de proceso.
- Entidades de vigilancia y control.
- Alcaldía de Bucaramanga.
- Proveedores de servicios tecnológicos.
- Proveedores con acceso a información institucional.
- Entidades públicas con las cuales se intercambia información.

Las necesidades y expectativas de estas partes interesadas se relacionan principalmente con la protección de los datos personales, disponibilidad de los servicios, integridad de la información, acceso autorizado, confidencialidad, transparencia y cumplimiento de los requisitos legales y contractuales aplicables.

7.2.3 Política de Seguridad y Privacidad de la Información

La Política de Seguridad y Privacidad de la Información constituye el marco directivo para la protección de los activos de información del INVISBU y deberá mantenerse articulada con el MSPI.

La política deberá ser formalmente aprobada y comunicada a funcionarios, contratistas y demás partes interesadas a las cuales resulte aplicable.

Acto administrativo de adopción: *Acta de Gestión y Desempeño – 31 enero 2026*.

7.2.4 Gestión de activos de información

El INVISBU mantiene un inventario de activos de información en el cual se identifican los activos, sistemas y servicios institucionales, sus responsables, ubicación, soporte y clasificación.

El inventario será actualizado cuando se presenten cambios significativos en los procesos, sistemas de información, infraestructura tecnológica, servicios o responsables.

Evidencia: Inventario de Activos de Información.

7.2.5 Clasificación de la información

La información será clasificada de acuerdo con su sensibilidad, uso, criticidad, restricciones legales y consecuencias derivadas de una eventual divulgación, alteración o indisponibilidad.

Para la gestión institucional se consideran los niveles definidos en el PSPI:

- Información pública.
- Información interna.
- Información reservada.
- Información confidencial.

La clasificación constituye un insumo para la asignación de permisos, definición de controles, gestión de riesgos y gestión de proveedores.

7.2.6 Gestión de riesgos

La gestión de riesgos de seguridad y privacidad se desarrolla a partir de los activos de información y la identificación de amenazas y vulnerabilidades, considerando criterios de probabilidad e impacto.

Los riesgos identificados serán valorados, priorizados y tratados mediante controles y acciones orientadas a evitar, reducir, transferir o aceptar el riesgo de acuerdo con los criterios institucionales.

La gestión se articulará con el mapa institucional de riesgos para evitar duplicidades y garantizar la trazabilidad de las acciones.

Evidencias:

- Matriz de Amenazas y Vulnerabilidades.
- Matriz de Riesgos de Seguridad y Privacidad de la Información.
- Plan de tratamiento de riesgos correspondiente.

7.2.7 Declaración de aplicabilidad

El INVISBU establecerá y mantendrá una **Declaración de Aplicabilidad**, mediante la cual se identificarán los controles de seguridad que resulten aplicables a la entidad, su estado de implementación, justificación de inclusión o exclusión y las evidencias asociadas.

La Declaración de Aplicabilidad será actualizada de acuerdo con los resultados de la gestión de riesgos, cambios institucionales y evolución del MSPI.

7.2.8 Cultura, sensibilización y apropiación

El INVISBU promoverá actividades de sensibilización y apropiación dirigidas a funcionarios y contratistas sobre aspectos tales como protección de datos personales, phishing, contraseñas y credenciales, uso seguro del correo electrónico, manejo de información institucional, reporte de incidentes y demás temas de seguridad relevantes.

Las actividades realizadas deberán conservar evidencia de su ejecución.

7.3 Fase de Operación

La fase de operación comprende la implementación de las medidas y controles definidos durante la planificación.

7.3.1 Implementación de controles

Los controles de seguridad serán implementados de manera proporcional a los riesgos identificados, la criticidad de los activos y las capacidades institucionales.

La implementación deberá conservar evidencias verificables tales como configuraciones, registros, actas, reportes, listados de accesos, informes técnicos, soportes de capacitación y demás documentos aplicables.

7.3.2 Gestión de accesos

La entidad establecerá mecanismos para la creación, modificación, revisión y retiro de permisos de acceso a sistemas, aplicaciones, correo electrónico, bases de datos y demás recursos institucionales.

Los permisos deberán responder a las funciones y responsabilidades de los usuarios y aplicar criterios de mínimo privilegio y necesidad de conocer.

7.3.3 Gestión de incidentes

Todos los eventos o incidentes que comprometan o puedan comprometer la confidencialidad, integridad, disponibilidad o privacidad de la información deberán ser reportados y gestionados.

La Oficina Asesora TIC coordinará su recepción, análisis, atención, contención, recuperación, documentación y cierre.

Los incidentes deberán conservarse en un registro institucional que permita identificar causas, controles afectados, acciones implementadas y lecciones aprendidas.

Cuando resulte legalmente obligatorio, los incidentes serán comunicados a las autoridades o instancias competentes.

7.3.4 Gestión de vulnerabilidades

La entidad realizará actividades orientadas a identificar y tratar vulnerabilidades de la infraestructura, equipos, sistemas y servicios tecnológicos bajo su alcance.

Las vulnerabilidades identificadas deberán analizarse de acuerdo con su nivel de riesgo y generar, cuando corresponda, actividades de actualización, configuración, corrección o mitigación.

7.3.5 Gestión de proveedores y terceros

Los proveedores que tengan acceso a sistemas, infraestructura o información institucional estarán sujetos a controles de seguridad proporcionales al servicio suministrado y al nivel de acceso concedido.

La entidad realizará revisiones periódicas de accesos, compromisos de confidencialidad y demás condiciones de seguridad aplicables.

7.3.6 Copias de seguridad

El INVISBU mantendrá mecanismos de respaldo de la información institucional de acuerdo con su criticidad.

Las copias de seguridad deberán contar con periodicidades, responsables, medios de almacenamiento y registros que permitan evidenciar su ejecución y facilitar la recuperación de la información cuando resulte necesario.

7.3.7 Continuidad y disponibilidad

La gestión de continuidad estará orientada a reducir los efectos de fallas tecnológicas, incidentes o eventos adversos que puedan afectar la prestación de servicios institucionales.

La entidad identificará los servicios y activos críticos y establecerá estrategias de recuperación proporcionales a sus necesidades y capacidades.

7.3.8 Servicios en nube

Los servicios en nube utilizados por la entidad deberán ser gestionados aplicando controles relacionados con acceso, autenticación, almacenamiento, intercambio, respaldo y protección de la información.

La Oficina Asesora TIC realizará seguimiento a las condiciones de seguridad de los servicios institucionales que operen bajo esta modalidad

.

7.3.9 Plan de Seguridad y Privacidad de la Información

El **PSPI 2026** constituye el instrumento operativo para ejecutar las actividades priorizadas del MSPI durante la vigencia.

El Plan de Acción asociado establece riesgos, actividades, responsables, apoyos, plazos y evidencias y permite efectuar seguimiento al avance de la implementación.

7.4 Fase de Evaluación del Desempeño

El INVISBU realizará el seguimiento y evaluación de la implementación del MSPI con el propósito de determinar su nivel de avance y la efectividad de las medidas implementadas.

7.4.1 Monitoreo, medición, análisis y evaluación

La Oficina Asesora TIC establecerá indicadores que permitan evaluar, entre otros aspectos:

- Avance del Plan de Acción del PSPI.
- Cumplimiento del plan de copias de seguridad.
- Gestión de incidentes de seguridad.
- Implementación de acciones de tratamiento de riesgos.
- Ejecución de actividades de sensibilización.
- Revisión de accesos y perfiles.
- Cumplimiento de controles relacionados con proveedores.

Los resultados serán documentados y utilizados para identificar desviaciones y oportunidades de mejora.

7.4.2 Evaluación independiente

La Oficina de Control Interno podrá incorporar dentro de sus actividades de evaluación y seguimiento la revisión del estado de implementación del MSPI, de acuerdo con su programación y competencias.

Los hallazgos y recomendaciones que se generen deberán ser analizados para determinar las acciones de mejora correspondientes.

7.4.3 Revisión por la Alta Dirección

Los resultados relevantes del MSPI serán presentados a la Alta Dirección y/o al Comité Institucional de Gestión y Desempeño para conocimiento, análisis y toma de decisiones.

La revisión podrá considerar:

- Estado del Plan de Acción.

- Riesgos relevantes.
- Incidentes presentados.
- Resultados de indicadores.
- Hallazgos de auditoría.
- Necesidades de recursos.
- Cambios normativos o tecnológicos.
- Acciones de mejora.

7.5 Fase de Mejoramiento Continuo

El INVISBU desarrollará acciones de mejora con fundamento en los resultados del seguimiento, indicadores, auditorías, incidentes, análisis de riesgos, cambios tecnológicos y revisiones institucionales.

Las desviaciones o debilidades identificadas deberán generar, según corresponda, acciones correctivas, preventivas o de mejora, indicando responsable, plazo y evidencia de cumplimiento.

Los resultados de esta fase constituirán insumo para actualizar el diagnóstico MSPI y establecer las prioridades de las siguientes vigencias, garantizando la continuidad del ciclo de mejoramiento.

8. ARTICULACIÓN DEL MSPI CON EL PSPI 2026

El MSPI constituye el **marco institucional de gestión de la seguridad y privacidad de la información**, mientras que el PSPI constituye el **instrumento de planificación y ejecución de las actividades priorizadas para cada vigencia**.

En consecuencia, ambos documentos son complementarios y no sustitutos.

Los resultados del diagnóstico MSPI alimentan la planificación del PSPI; las actividades del PSPI permiten implementar controles y cerrar brechas; y los resultados de seguimiento permiten evaluar nuevamente el estado del MSPI y establecer nuevas acciones de mejora.

9. DOCUMENTACIÓN Y EVIDENCIAS DEL MSPI

La implementación del Modelo se soportará, entre otros, en los siguientes documentos e instrumentos:

1. Documento Marco del Modelo de Seguridad y Privacidad de la Información – MSPI.
2. Política de Seguridad y Privacidad de la Información.
3. Plan de Seguridad y Privacidad de la Información – PSPI.
4. Autodiagnóstico MSPI.
5. Inventario y clasificación de activos de información.
6. Matriz de amenazas y vulnerabilidades.
7. Matriz de riesgos de seguridad y privacidad de la información.
8. Plan de tratamiento de riesgos.
9. Declaración de Aplicabilidad.

10. Lineamientos o manual de políticas de seguridad.
11. Registros de gestión de incidentes.
12. Plan y registros de copias de seguridad.
13. Evidencias de revisión de accesos.
14. Evidencias de sensibilización y capacitación.
15. Indicadores y registros de seguimiento.
16. Informes de evaluación o auditoría.
17. Registros de acciones correctivas y de mejora.

Los documentos podrán mantenerse de manera independiente y serán actualizados de acuerdo con los cambios institucionales, tecnológicos, normativos y de riesgos.

10. SEGUIMIENTO DEL MSPI

La Oficina Asesora TIC realizará seguimiento periódico al estado de implementación del MSPI y al cumplimiento del PSPI.

Como mínimo, se deberá verificar:

- Avance de las acciones programadas.
- Implementación de controles.
- Estado de los riesgos.
- Incidentes registrados.
- Cumplimiento de actividades de respaldo.
- Gestión de proveedores.
- Actividades de sensibilización.
- Indicadores establecidos.
- Acciones correctivas y oportunidades de mejora.

Los resultados servirán de insumo para la toma de decisiones y la actualización del modelo.

11. RESPONSABLES

Alta Dirección: respaldo institucional, orientación estratégica y asignación de recursos.
Comité Institucional de Gestión y Desempeño: seguimiento y toma de decisiones relacionadas con el MSPI dentro de sus competencias.
Oficina Asesora TIC: liderazgo técnico, coordinación, implementación, seguimiento y gestión de seguridad tecnológica.
Líderes de proceso: gestión y protección de los activos y riesgos asociados a sus procesos.
Oficina de Control Interno: evaluación independiente.
Funcionarios y contratistas: cumplimiento de las políticas, controles y lineamientos institucionales.
Proveedores: cumplimiento de los requisitos contractuales y controles de seguridad aplicables al servicio prestado.

12. DOCUMENTOS COMPLEMENTARIOS Y ANEXOS DEL MSPI

La implementación del Modelo de Seguridad y Privacidad de la Información – MSPI del INVISBU se soporta en los siguientes documentos e instrumentos, los cuales se gestionan y actualizan de manera independiente de acuerdo con su naturaleza, periodicidad y nivel de clasificación:

Anexo 1. Matriz de Autodiagnóstico MSPI – Base 2026.

Anexo 2. Inventario de Activos de Información.

Anexo 3. Matriz de Amenazas y Vulnerabilidades.

Anexo 4. Matriz de Riesgos de Seguridad y Privacidad de la Información.

Anexo 5. Plan de Seguridad y Privacidad de la Información – PSPI 2026 y su Plan de Acción.

Anexo 6. Declaración de Aplicabilidad.

Anexo 7. Indicadores del MSPI.

Estos documentos constituyen evidencia de la implementación y seguimiento del MSPI y podrán ser actualizados de manera independiente, conservando su trazabilidad, control de versiones y articulación con el presente Modelo.

La publicación o divulgación de estos documentos se realizará de acuerdo con su clasificación y con las disposiciones aplicables en materia de transparencia, acceso a la información, protección de datos personales y seguridad de la información.

13. APROBACIÓN Y ACTUALIZACIÓN

El Modelo de Seguridad y Privacidad de la Información será revisado periódicamente y cuando se presenten cambios significativos en:

- La normatividad aplicable.
- Los procesos institucionales.
- La infraestructura tecnológica.
- Los sistemas de información.
- Los riesgos de seguridad y privacidad.
- Los servicios contratados con terceros.
- Los resultados de auditorías o evaluaciones.
- Los lineamientos emitidos por MinTIC.

Su implementación será objeto de mejoramiento continuo de acuerdo con las capacidades y prioridades institucionales.

Control de documentos

Elaboró: Oficina Asesora TIC – INVISBU	**Aprobó:** Comité Institucional de Gestión y Desempeño	**FECHA DE APROBACIÓN:** Enero 2026