POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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

Versión: 01
Fecha: enero 2026

1. OBJETIVO

Establecer los lineamientos, responsabilidades y directrices que orientan la protección, gestión y uso adecuado de la información del INVISBU, garantizando su confidencialidad, integridad, disponibilidad y privacidad, así como el cumplimiento de las normas vigentes en materia de seguridad digital, protección de datos personales y Gobierno Digital.

La presente Política se adopta en el marco del **Modelo de Seguridad y Privacidad de la Información – MSPI**, definido por el Ministerio de Tecnologías de la Información y las Comunicaciones, y se articula con el **Modelo Integrado de Planeación y Gestión – MIPG**, como parte del fortalecimiento del Sistema de Control Interno del INVISBU.

El INVISBU se compromete con la implementación, mantenimiento y mejora continua de los controles, procesos y mecanismos establecidos para la gestión de la seguridad y privacidad de la información, de acuerdo con los riesgos, capacidades institucionales y requisitos aplicables.

---

2. ALCANCE

La presente política aplica a:

- Funcionarios de planta
- Contratistas y prestadores de servicios
- Pasantes y personal temporal
- Proveedores con acceso a información institucional

Cubre todos los procesos, sistemas de información, equipos y activos tecnológicos del INVISBU, así como la información gestionada en medios físicos o digitales, independientemente de su formato o ubicación.

---

3. MARCO NORMATIVO

La presente Política se fundamenta, entre otras, en 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 1074 de 2015, en lo relacionado con protección de datos personales.
- Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector TIC y sus modificaciones.
- Decreto 338 de 2022 – Lineamientos generales para fortalecer la gobernanza de la seguridad digital.
- Decreto 767 de 2022 – Política de Gobierno Digital.
- 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 del Modelo de Seguridad y Privacidad de la Información – MSPI vigente.
- Modelo Integrado de Planeación y Gestión – MIPG.
- Norma ISO/IEC 27001:2022, como referente de buenas prácticas.
- Lineamientos, políticas, procedimientos y demás instrumentos internos del INVISBU

---

4. PRINCIPIOS DE SEGURIDAD Y PRIVACIDAD

Confidencialidad: La información será accesible únicamente a personas autorizadas.

Integridad: La información deberá mantenerse completa, exacta y protegida contra modificaciones no autorizadas.

Disponibilidad: La información estará disponible cuando sea requerida para el cumplimiento de las funciones institucionales.

Legalidad: El tratamiento de la información cumplirá estrictamente la normatividad vigente.

Autenticidad: Se garantizará la identidad y veracidad de usuarios, documentos y procesos.

Trazabilidad: Las actividades sobre la información deberán ser auditables.

---

5. LINEAMIENTOS GENERALES

5.1 Gestión de la información

La información generada, recibida, procesada, almacenada o custodiada por el INVISBU constituye un activo de información que deberá ser gestionado y protegido de acuerdo con su naturaleza, clasificación, criticidad y requisitos legales aplicables.

La información debe clasificarse como **pública, interna, reservada o confidencial**.

La clasificación de la información será responsabilidad de cada **líder de proceso**, con el acompañamiento de la **Oficina Asesora TIC**, conforme a los lineamientos definidos en el PSPI y el inventario de activos de información.

Se prohíbe eliminar, manipular o divulgar información sin autorización.

5.2 Protección de datos personales

El INVISBU garantiza el tratamiento adecuado de datos personales según la Ley 1581.

Los funcionarios y contratistas deberán proteger especialmente la información que contenga datos sensibles.
Se prohíbe copiar o transportar datos personales en dispositivos no autorizados.

5.3 Uso de equipos y recursos tecnológicos

Los equipos institucionales se usarán exclusivamente para fines laborales.

Está prohibida la instalación de software no autorizado o la conexión de hardware externo sin autorización.

El usuario es responsable de la custodia del equipo y de sus credenciales de acceso.

Queda prohibido utilizar los recursos tecnológicos, equipos, servicios e insumos institucionales para fines personales, comerciales o diferentes al cumplimiento de las funciones, obligaciones o actividades institucionales, salvo autorización expresa de la entidad.

5.4 Correo electrónico institucional

El correo institucional deberá utilizarse únicamente para funciones laborales.

No se deben abrir enlaces o archivos sospechosos.

Está prohibido compartir la contraseña o permitir el acceso de terceros.

El correo institucional es un medio oficial de comunicación y archivo.

5.5 Manejo de contraseñas

Las credenciales de acceso son personales, confidenciales e intransferibles.

Las contraseñas deberán cumplir los requisitos de longitud, complejidad y seguridad definidos por el INVISBU y por las plataformas o sistemas de información institucionales.

Está prohibido compartir contraseñas, permitir su utilización por terceros o almacenarlas sin las medidas de protección correspondientes.

Las contraseñas deberán ser modificadas cuando exista sospecha o evidencia de compromiso, cuando así lo requiera el sistema o cuando sea determinado por la Oficina Asesora TIC como medida de seguridad.

Cuando las plataformas institucionales lo permitan y de acuerdo con el nivel de riesgo, podrán implementarse mecanismos adicionales de autenticación para fortalecer la protección de las cuentas de usuario.

.

5.6 Seguridad en la red y navegación.

- La navegación deberá realizarse únicamente en sitios de confianza.
- Está prohibido desactivar herramientas de seguridad como antivirus o firewall.
- El acceso a la red institucional debe realizarse desde equipos autorizados.

5.7 Respaldo y recuperación de información

- Los respaldos se realizarán conforme al Plan de Backups del INVISBU.
- Se prohíbe almacenar documentos institucionales únicamente en equipos personales.
- La información institucional deberá almacenarse y respaldarse mediante los sistemas, repositorios, servicios en nube y demás mecanismos autorizados por el INVISBU.
- Los funcionarios y contratistas deberán utilizar los mecanismos institucionales definidos para el almacenamiento, transferencia, respaldo y entrega de archivos, evitando mantener la única copia de información institucional en equipos personales, dispositivos no autorizados o servicios particulares de almacenamiento.
- Cualquier pérdida, daño o alteración de información deberá ser reportada de inmediato.

5.8 Gestión y reporte de incidentes de seguridad de la información

Todo funcionario, contratista, pasante, proveedor o tercero que tenga acceso a información o recursos tecnológicos del INVISBU deberá reportar oportunamente cualquier evento o incidente que pueda comprometer la confidencialidad, integridad, disponibilidad o privacidad de la información.

Entre los eventos que deberán reportarse se encuentran, entre otros:

• Correos de phishing o comunicaciones sospechosas.
• Accesos no autorizados.
• Pérdida, alteración o divulgación no autorizada de información.
• Compromiso de credenciales.
• Infección por software malicioso.
• Pérdida, hurto o daño de equipos institucionales.
• Indisponibilidad anormal de sistemas o servicios tecnológicos.

El reporte se realizará a través de los canales definidos y divulgados por la Oficina Asesora TIC. Los incidentes serán gestionados y documentados de acuerdo con los lineamientos institucionales establecidos para tal efecto.

5.9 Acceso a los sistemas de información

- Se otorgará acceso de acuerdo con el rol y función del usuario.
- Queda prohibido acceder a información sin autorización.
- La Oficina Asesora TIC podrá suspender, modificar o retirar accesos cuando se presente terminación o suspensión de la relación laboral o contractual, cambio de funciones o responsabilidades, pérdida de la necesidad de acceso, solicitud del líder responsable, identificación de un riesgo o incidente de seguridad, o cualquier otra circunstancia debidamente justificada que pueda comprometer la seguridad de la información.

5.10 Responsabilidades del usuario

Todo usuario debe:

- Cumplir esta Política y las directrices del área TIC.
- Usar adecuadamente los activos tecnológicos asignados.
- Mantener la confidencialidad de la información.
- Reportar incidentes de seguridad.
- Proteger datos personales y sensibles.
- Participar en actividades de sensibilización institucional.

5.11 Seguridad de proveedores y terceros

Los contratos, convenios u otros instrumentos mediante los cuales terceros tengan acceso a información, sistemas, infraestructura o servicios tecnológicos del INVISBU deberán contemplar, de acuerdo con su naturaleza y nivel de riesgo, obligaciones relacionadas con confidencialidad, protección de datos personales, gestión de accesos, reporte de incidentes y demás controles de seguridad aplicables.

Los accesos concedidos a proveedores y terceros deberán limitarse a los recursos necesarios para el cumplimiento de sus obligaciones y serán revisados, modificados o retirados cuando corresponda.

5.12 Continuidad y disponibilidad de la información

El INVISBU implementará medidas orientadas a mantener y recuperar oportunamente la disponibilidad de la información y de los servicios tecnológicos críticos ante fallas, incidentes o eventos adversos, de acuerdo con los riesgos identificados, la criticidad de los servicios y las capacidades institucionales.

Estas medidas se articularán con el Plan de Copias de Seguridad, la gestión de incidentes, la gestión de riesgos y los demás instrumentos institucionales aplicables.

---

6. ROLES Y RESPONSABILIDADES

Alta Dirección

• Brindar respaldo institucional a la implementación de la presente Política y propiciar la disponibilidad de los recursos requeridos para la gestión de la seguridad y privacidad de la información.

Comité Institucional de Gestión y Desempeño

• Orientar y realizar seguimiento, en el marco de sus competencias, a la implementación de la Política de Seguridad y Privacidad de la Información.

• Aprobar la Política y sus actualizaciones, de acuerdo con las competencias institucionales.

• Conocer los resultados relevantes relacionados con la implementación del MSPI y adoptar las decisiones que correspondan.

Oficina Asesora TIC

• Liderar técnicamente la implementación del MSPI y del PSPI.

• Coordinar la implementación de controles tecnológicos de seguridad.

• Gestionar los incidentes de seguridad de la información.

• Realizar seguimiento a las actividades de seguridad y privacidad bajo su responsabilidad.

Líderes de proceso

• Identificar, custodiar y clasificar los activos de información bajo su responsabilidad.

• Participar en la identificación y tratamiento de riesgos de seguridad y privacidad de la información.

• Velar por la aplicación de los lineamientos establecidos en la presente Política dentro de sus procesos.

Oficina de Control Interno

• Realizar la evaluación independiente de la implementación y efectividad de las medidas de seguridad y privacidad de la información, en el marco de sus competencias.

Funcionarios, contratistas, pasantes y proveedores

• Cumplir la presente Política y demás lineamientos institucionales aplicables.

• Proteger la información a la cual tengan acceso.

• Reportar oportunamente eventos o incidentes de seguridad de la información.

---

7. DIVULGACIÓN Y SENSIBILIZACIÓN

El INVISBU realizará actividades de socialización, capacitación y divulgación de la presente Política a través de medios institucionales.

---

8. VIGENCIA, REVISIÓN Y ACTUALIZACIÓN

La presente Política de Seguridad y Privacidad de la Información fue aprobada por el Comité Institucional de Gestión y Desempeño del INVISBU, mediante Acta de fecha 31 de enero de 2026, y rige a partir de su aprobación.

La Política será revisada como mínimo una vez al año o 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 de la información o los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

Las modificaciones que se deriven de dicha revisión deberán conservar la correspondiente trazabilidad y control de cambios.

Campo	Información
Documento	Política de Seguridad y Privacidad de la Información
Versión	1.0
Vigencia	2026
Elaboró	Oficina Asesora TIC – INVISBU
Aprobó	Comité Institucional de Gestión y Desempeño
Fecha de aprobación	31 de enero de 2026
Evidencia de aprobación	Acta del Comité Institucional de Gestión y Desempeño del 31 de enero de 2026