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

---

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:

- Constitución Política de Colombia – Artículo 15
- Ley 1581 de 2012 – Protección de Datos Personales
- Ley 1712 de 2014 – Transparencia y Acceso a la Información Pública
- Ley 594 de 2000 – Ley General de Archivos
- Ley 1273 de 2009 – Protección de la Información y los Datos
- Decreto 1078 de 2015 – Sector TIC
- Decreto 1008 de 2018 – Gobierno Digital
- Lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI
- Norma ISO/IEC 27001 (como referencia de buenas prácticas)
- Lineamientos internos y manuales institucionales 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

Toda información institucional es un activo del INVISBU.
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 estrictamente prohibido, especialmente para el personal contratista, el uso de los recursos tecnológicos e insumos institucionales (tales como impresoras de red, impresoras de inyección de tinta como las Epson EcoTank L3250, quemadoras de CD, papel y tóner) para la generación, impresión o reproducción de sus cuentas de cobro, anexos de facturación o cualquier otro documento de carácter personal o comercial.

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 contraseñas deberán ser personales, seguras y confidenciales.

Deben ser robustas, exigiendo una longitud mínima de diez (10) caracteres que incluyan una combinación de letras (mayúsculas y minúsculas), números y caracteres especiales.

No deben compartirse ni almacenarse sin medidas de protección y deberán cambiarse periódicamente.

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.
- En concordancia con el enfoque de austeridad y uso de herramientas de nube institucional, los funcionarios de planta deberán utilizar la unidad de 1 Terabyte (1TB) asignada en su OneDrive for Business para salvaguardar la información.
- Para el caso de los contratistas de prestación de servicios, el respaldo y entrega de archivos pesados se realizará obligatoriamente mediante enlaces de "Solicitud de Archivos" hacia carpetas institucionales, asegurando así la integridad de la información sin colapsar el almacenamiento del servidor.
- Cualquier pérdida, daño o alteración de información deberá ser reportada de inmediato.

5.8 Incidentes de seguridad

Todo funcionario debe reportar inmediatamente incidentes como:

- Todo funcionario debe reportar inmediatamente incidentes como: Phishing o correos maliciosos, pérdida de información, accesos indebidos, infección por malware, y pérdida o daño de equipos. Pérdida de información.
- El reporte se realizará a través de los canales definidos por la Oficina Asesora TIC, los cuales serán divulgados institucionalmente.

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.
- TIC podrá revocar accesos cuando lo considere necesario para la seguridad.

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.

---

6. ROLES Y RESPONSABILIDADES

Dirección General

- Aprobar la Política y garantizar los recursos necesarios.

Oficina Asesora TIC

- Coordinar la implementación del MSPI y PSPI, administrar la seguridad tecnológica y gestionar incidentes.

Líderes de proceso

- Velar por el cumplimiento de la Política en sus áreas y clasificar la información del proceso.

Funcionarios y contratistas: Cumplir integralmente la Política y reportar incidentes.

Proveedores: Cumplir los acuerdos de confidencialidad y protección 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

La presente Política será aprobada y adoptada y será revisada anualmente o cuando existan cambios normativos o tecnológicos relevantes.

Rubith López Palomino – Asesor TIC