MODELO Y PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) - INVISBU

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

Responsables: Comité de Gobierno Digital / Oficina TIC
Vigencia: 2025

1. OBJETIVO

Establecer el marco de protección para los activos de información del Instituto, garantizando la confidencialidad, integridad y disponibilidad de los datos de los beneficiarios de programas de vivienda, bajo un enfoque de austeridad y eficiencia administrativa.

2. ALCANCE

Aplica a todos los procesos misionales (Subsidios, Mejoramiento, Jurídica, Técnica) y de apoyo que utilizan el ecosistema digital del Instituto, los servidores *on-premise* y las herramientas de nube institucional.

3. INVENTARIO DE ACTIVOS CRÍTICOS (2025)

La seguridad de la información se centra en proteger los siguientes pilares tecnológicos:

- **SIGAPI (Plataforma Institucional):** Sistema desarrollado a medida que centraliza la atención y gestión de la población.
- **Servidor Linux:** Aloja el motor de base de datos y el repositorio central de archivos del SIGAPI.
- **Servidor Windows Server:** Soporta los servicios administrativos y de red interna.
- **Correo Institucional:** Canales @invisbu.gov.co (M365) y @ctinvisbu.gov.co (Hosting IMAP).

4. GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

Bajo el modelo **MSPI**, el Instituto gestiona los riesgos de su infraestructura *on-premise* mediante los siguientes controles:

4.1 Control de Acceso Lógico

- **Uso de Roles:** El acceso al SIGAPI está restringido estrictamente por perfiles (Administrador, Funcionario, Contratista) vinculados a la vigencia del contrato o vinculación laboral.
- **Autenticación:** Uso obligatorio de contraseñas robustas de mínimo 10 caracteres, combinando mayúsculas, minúsculas, números y símbolos.
- **Cierre de Sesión:** Obligatoriedad de cerrar sesiones al finalizar la jornada para evitar accesos no autorizados en los puestos de trabajo.

4.2 Seguridad Operativa y Respaldo

- **Estrategia de Respaldo (Backup):** Realización de *dumps* periódicos de la base de datos en el servidor Linux y copia del repositorio de archivos hacia la nube institucional.
- **Capacidad de Nube:** El personal de planta utiliza **1TB** de OneDrive para asegurar que la información misional sea recuperable ante fallos de hardware local.

- **Gestión de Contratistas:** Uso de enlaces de **"Solicitud de Archivos"** en OneDrive para recibir planos e informes pesados, evitando la saturación del hosting IMAP y garantizando la integridad de los entregables.

5. PROTECCIÓN DE DATOS PERSONALES (LEY 1581 DE 2012)

El SIGAPI integra la privacidad desde el diseño para proteger a la población vulnerable:

- **Autorización Expresa:** Todo trámite digital requiere la autorización del tratamiento de datos y la aceptación del aviso de privacidad.
- **Validación de Identidad:** El sistema verifica automáticamente números de cédula para evitar registros duplicados y suplantación en los trámites de subsidios.
- **Transparencia Activa:** Publicación de noticias y catálogos de servicios actualizados en tiempo real para garantizar el derecho a la información de la ciudadanía.

6. CULTURA Y SENSIBILIZACIÓN

Ante la restricción presupuestal para hardware especializado, el **INVISBU** prioriza el factor humano como primera línea de defensa:

- **Capacitación Obligatoria:** El **100%** del personal administrativo y operativo debe completar anualmente el ciclo de capacitación en seguridad digital y uso adecuado del SIGAPI.
- **Prevención de Phishing:** Jornadas de sensibilización sobre riesgos en correos externos para verificar la coherencia de remitentes antes de descargar anexos.

7. MONITOREO Y MEJORA CONTINUA (MIPG)

- **Tableros de Indicadores:** Uso de los tableros del SIGAPI para monitorear métricas de atención y seguridad en tiempo real, asegurando decisiones basadas en evidencia técnica.

- **Evaluación FURAG:** Medición anual del Índice de Desempeño Institucional en las políticas de Gobierno Digital y Seguridad Digital para identificar brechas y oportunidades de mejora.

Nota Metodológica: Este modelo se operativiza mediante el Plan de Recuperación de Desastres (DRP) y el Plan de Continuidad del Negocio (BCP) aprobados para la vigencia 2025.