POLÍTICA DE SEGURIDAD DIGITAL Y DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

El Instituto de Vivienda de Interés Social y Reforma Urbana del Municipio de Bucaramanga (INVISBU) reconoce la importancia estratégica de proteger sus activos de información y sistemas tecnológicos para garantizar la continuidad de sus procesos misionales orientados a la provisión de soluciones habitacionales y desarrollo urbano.

Esta política se enmarca en el cumplimiento de la normatividad vigente y adopta las mejores prácticas en seguridad digital establecidas por el Gobierno Nacional.

2. MARCO NORMATIVO

La presente política se fundamenta en:

- Decreto 767 de 2022: Lineamientos generales de la Política de Gobierno Digital.
- Resolución 746 de 2022: Fortalecimiento del Modelo de Seguridad y Privacidad de la Información.
- Resolución 500 de 2021: Lineamientos y estándares para la estrategia de seguridad digital.
- CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital.
- CONPES 3854 de 2016: Política Nacional de Seguridad Digital.
- Ley 1581 de 2012: Ley de Protección de Datos Personales.
- Decreto 1078 de 2015: Decreto Único Reglamentario del Sector TIC.

3. OBJETIVO GENERAL

Establecer el marco institucional para la gestión integral de la seguridad digital y de la información en INVISBU, garantizando la confidencialidad, integridad y disponibilidad de los activos de información que soportan los procesos misionales, administrativos y estratégicos de la entidad.

4. OBJETIVOS ESPECÍFICOS

- Implementar el Modelo de Seguridad y Privacidad de la Información (MSPI) conforme a los lineamientos de MinTIC.
- Establecer controles técnicos, administrativos y de talento humano para la protección de activos de información.

- Desarrollar una cultura organizacional de seguridad digital a través de programas de sensibilización y capacitación.
- Gestionar sistemáticamente los riesgos de seguridad digital mediante metodologías de identificación, evaluación y tratamiento.
- Garantizar el cumplimiento normativo en materia de protección de datos personales y seguridad de la información.

5. ALCANCE Y ÁMBITO DE APLICACIÓN

Esta política aplica a:

5.1. Personal Cubierto

- Todos los funcionarios públicos de INVISBU.
- Contratistas y personal de apoyo.
- Proveedores y terceros que accedan a información institucional.
- Visitantes que utilicen recursos tecnológicos de la entidad.

5.2. Activos Incluidos

- Información en formato físico y digital.
- Sistemas de información y bases de datos.
- Infraestructura tecnológica (servidores, equipos de comunicación, dispositivos móviles).
- Software y licencias.
- Instalaciones y espacios físicos donde se procesa información.

6. PRINCIPIOS FUNDAMENTALES

6.1. Confidencialidad

Garantizar que la información sea accesible únicamente por personas autorizadas según su rol y necesidades funcionales.

6.2. Integridad

Asegurar la exactitud y completitud de la información y los métodos de procesamiento durante todo su ciclo de vida.

6.3. Disponibilidad

Garantizar que los usuarios autorizados tengan acceso a la información y activos asociados cuando lo requieran.

6.4. Legalidad

Cumplir con toda la normatividad aplicable en materia de protección de datos, transparencia y acceso a la información pública.

7. ESTRUCTURA DE GOBIERNO DE SEGURIDAD

7.1. Alta Dirección

- Director General de INVISBU: Responsable del respaldo institucional y asignación de recursos.
- Comité Institucional de Gestión y Desempeño: Seguimiento y evaluación de la política.

7.2. Nivel Operativo

- Responsable de Seguridad Digital: Coordinación de la implementación del MSPI.
- Líderes de proceso: Aplicación de controles en sus áreas respectivas.
- Oficina de Control Interno: Verificación del cumplimiento y auditorías periódicas.

8. ESTRATEGIAS Y DIMENSIONES DE SEGURIDAD

8.1. Liderazgo en Seguridad

Establecimiento de responsabilidades claras desde la alta dirección para garantizar recursos, apoyo estratégico y toma de decisiones alineadas con los objetivos institucionales.

8.2. Gestión de Riesgos

Implementación de un proceso sistemático y cíclico para identificar, evaluar, tratar y monitorear los riesgos de seguridad digital que puedan afectar los activos de información.

8.3. Implementación de Controles

Adopción de medidas técnicas, administrativas y físicas para proteger los activos de información, incluyendo:

- Controles de acceso basados en roles.
- Sistemas de detección y prevención de intrusiones.
- Copias de seguridad y planes de recuperación.
- Actualizaciones de seguridad y gestión de parches.

8.4. Cultura y Concientización

Desarrollo de programas continuos de capacitación y sensibilización dirigidos a todos los niveles organizacionales para promover buenas prácticas de seguridad.

8.5. Gestión de Incidentes

Establecimiento de procedimientos claros para la identificación, notificación, clasificación y resolución de incidentes de seguridad, garantizando respuesta oportuna y efectiva.

9. RESPONSABILIDADES ESPECÍFICAS

9.1. De la Alta Dirección

- Aprobar y respaldar la política de seguridad digital.
- Asignar recursos necesarios para la implementación.
- Revisar periódicamente la efectividad de los controles.

9.2. Del Responsable de Seguridad Digital

- Coordinar la implementación del MSPI.
- Realizar seguimiento a indicadores de seguridad.
- Reportar incidentes y vulnerabilidades a la alta dirección.

9.3. De los Funcionarios y Contratistas

- Cumplir con las políticas y procedimientos establecidos.
- Reportar incidentes de seguridad de manera oportuna.
- Participar en programas de capacitación y sensibilización.

10. PROCEDIMIENTOS ESPECÍFICOS

10.1. Clasificación de la Información

Toda información institucional debe clasificarse según su nivel de sensibilidad:

- Pública: Sin restricciones de acceso.
- Clasificada: Acceso restringido según normativa.
- Reservada: Máximo nivel de protección.

10.2. Gestión de Accesos

- Implementación de controles de acceso basados en roles.
- Revisión periódica de permisos y privilegios.
- Procedimientos de alta, modificación y baja de usuarios.

10.3. Respuesta a Incidentes

- Detección y notificación inmediata de incidentes.
- Evaluación y clasificación según impacto y urgencia.
- Respuesta coordinada entre áreas involucradas.
- Análisis post-incidente para mejora continua.

11. INDICADORES DE GESTIÓN

INVISBU implementará indicadores para medir la efectividad de la política, incluyendo:

- Índice de madurez del Sistema de Gestión de Seguridad.

- Tiempo promedio de respuesta a incidentes.
- Porcentaje de personal capacitado anualmente.
- Nivel de cumplimiento de controles implementados.

12. REVISIÓN Y ACTUALIZACIÓN

Esta política será revisada anualmente o cuando se presenten cambios significativos en:

- Marco normativo aplicable.
- Tecnología utilizada por la entidad.
- Estructura organizacional.
- Amenazas del entorno digital.

13. SANCIONES Y CONSECUENCIAS

El incumplimiento de esta política puede generar:

- Medidas disciplinarias según el régimen aplicable.
- Terminación de contratos para proveedores y contratistas.
- Responsabilidades civiles y penales según la legislación vigente.

14. COMUNICACIÓN

Esta política debe ser socializada, implementada y monitoreada de manera continua para garantizar la protección efectiva de los activos de información de INVISBU y el cumplimiento de su misión institucional en beneficio de la comunidad bumanguesa.