INTRODUCCIÓN

La Política de Seguridad Digital del Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo – IMVIYUMBO, establece el marco estratégico y operativo para proteger la información, los activos tecnológicos y los servicios digitales que soportan la gestión institucional. Esta política busca garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de los datos, así como la resiliencia frente a incidentes y amenazas en el entorno digital.

En concordancia con las disposiciones nacionales en materia de ciberseguridad y seguridad de la información, el Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo – IMVIYUMBO asume el compromiso de implementar medidas preventivas y correctivas que minimicen los riesgos asociados al uso de las Tecnologías de la Información y las Comunicaciones (TIC), asegurando que los procesos internos y los servicios a la ciudadanía se desarrollen de manera confiable y segura.

La transformación digital trae consigo grandes oportunidades para optimizar la gestión pública, pero también nuevos retos frente a ataques cibernéticos, pérdida de datos o uso indebido de la información. Por ello, el Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo – IMVIYUMBO considera la seguridad digital como un pilar fundamental para el fortalecimiento institucional, la transparencia y la confianza de los ciudadanos en los servicios que ofrece.

OBJETIVO GENERAL

Fortalecer la capacidad para reconocer, gestionar y aminorar de forma efectiva los riesgos de seguridad digital que puedan salir durante el desarrollo de actividades cotidianas en entornos digitales por medio de herramientas tecnológicas, fomentando no solo la transparencia y el acceso a la información, sino también mejorando la calidad de los servicios públicos digitales y garantizar un acceso inclusivo.

OBJETIVOS ESPECÍFICOS.

- ✓ Establecer procedimientos efectivos, eficaces y eficientes para mitigar el impacto de los incidentes de seguridad digital y ciberataques.
- ✓ Facilitar y formalizar la gestión integral de los riesgos de seguridad digital (ciberseguridad) para que sean conocidos, valorados y tratados de manera eficiente.
- ✓ Garantizar la continuidad de la operación institucional y la disponibilidad de los sistemas de información críticos ante eventos adversos.
- ✓ Asegurar que la información sensible solo sea accedida por individuos, entidades o procesos autorizados.
- ✓ Definir e implementar los lineamientos, procedimientos y controles necesarios para proteger los activos de información (hardware, software, datos, personas) y los servicios tecnológicos.
- ✓ Definir, precisar y formalizar los elementos normativos internos sobre la protección de la información y la seguridad digital.
- ✓ Asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales vigentes en materia de seguridad y privacidad de la información (ej. leyes de protección de datos personales).
- ✓ Fomentar una cultura de seguridad digital en todos los empleados, contratistas y terceros, generando un cambio organizacional a través de la formación y sensibilización.
- ✓ Evaluar periódicamente los riesgos y actualizar las medidas de protección según la evolución tecnológica.

ALCANCE

La Política de Seguridad Digital y Privacidad de la información del Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo – IMVIYUMBO, aplica a todos los procesos, empleados, contratistas, proveedores, operadores, entes de control y demás terceros que en el ejercicio de sus funciones, obligaciones, compartan, utilicen, recolecten, procesen, intercambien o consulten los activos de información, tanto de manera interna como externa.

MARCO NORMATIVO

- ✓ Constitución Política de Colombia (1991) – Artículos 15 y 20 (protección de datos e información).
- ✓ Ley 1273 de 2009 – Protección de la información y de los datos. “Por medio de la cual se modifica el Código Penal, se crea un nuevo Bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"
- ✓ Ley 1581 de 2012 – Protección de datos personales. también conocida como la Ley de Protección de Datos Personales en Colombia, establece los principios y mecanismos para garantizar el derecho fundamental de las personas a conocer, actualizar y rectificar la información que se encuentra en bases de datos o archivos. Esta ley busca proteger la privacidad y los datos personales de los ciudadanos frente a tratamientos indebidos por parte de entidades públicas y privadas.
- ✓ Ley 1712 de 2014 – Transparencia y acceso a la información pública. también conocida como la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, regula el acceso a la información pública en Colombia. Establece el derecho de todas las personas a solicitar y recibir información en poder de entidades públicas, sin necesidad de justificar la solicitud. La ley busca garantizar la transparencia y el acceso a la información pública, así como los procedimientos para ejercer este derecho y las excepciones a la publicidad de la información.
- ✓ Decreto 1008 de 2018 – Política de Gobierno Digital (componente de seguridad digital). Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de las Tecnologías de la Información y las Comunicaciones.
- ✓ Normas ISO/IEC 27001, 27002 y 22301 – Seguridad de la información y continuidad del negocio.
- ✓ Guías y lineamientos del Ministerio TIC y ColCERT sobre ciberseguridad y gestión de incidentes.

DECLARACIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo IMVIYUMBO reconoce y es consciente de la importancia crucial de sus activos de información en todos sus procesos. Estos activos son fundamentales para la formulación, implementación, coordinación y evaluación de políticas, planes, programas y proyectos dirigidos a avanzar en la garantía del derecho a la igualdad y la equidad para todas las personas, especialmente de los sujetos de especial protección constitucional.

Por lo cual IMVIYUMBO se compromete con la adopción, implementación, mantenimiento y mejora continua de su Plan de Seguridad y Privacidad de la Información (PSPI). Este plan es esencial, ya que establece los lineamientos de seguridad y privacidad necesarios para generar un marco de confianza en el ejercicio de su misión, tanto con los sujetos de especial protección constitucional como con el Estado.

PRINCIPIOS FUNDAMENTALES DE LA SEGURIDAD DIGITAL.

El Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo IMVIYUMBO, basa su estrategia de seguridad en los siguientes principios:

- 🔒 Confidencialidad. Garantizar que la información solo sea accesible por aquellos individuos, entidades o procesos que tienen autorización.

- ✅ Integridad. Asegurar la exactitud, completitud y validez de la información y sus métodos de procesamiento, protegiéndola contra modificaciones no autorizadas.

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

-  Cumplimiento. Garantizar el acatamiento de leyes, regulaciones y obligaciones contractuales relacionadas con la seguridad digital y la protección de datos.

DIRECTRICES GENERALES DE LA POLÍTICA.

Gestión del riesgo y continuidad.

Se establecerá e implementará un Modelo de Gestión de Riesgos de Seguridad Digital para identificar, evaluar, tratar y monitorear los riesgos a los activos de información.

Para lo cual el instituto adopta un enfoque integral de gestión de riesgos, basado en las siguientes actividades:

1. Identificación de amenazas y vulnerabilidades.
2. Análisis de amenazas y vulnerabilidades.
3. Tratamiento de amenazas y vulnerabilidades.
4. Monitoreo de amenazas y vulnerabilidades.

El propósito de este enfoque es garantizar la resiliencia institucional frente a posibles incidentes de seguridad. Así mismo establecer e implementar diversos controles para fortalecer su seguridad digital y operativa:

- 🚪 Controles físicos.
- 📝 Controles administrativos.
- 🖥️ Controles tecnológicos.

Si la integridad de un sistema se ve comprometida, la información puede ser manipulada, llevando a decisiones erróneas, fraude o pérdida de confianza

Lo anterior asegura el cumplimiento de requisitos legales, normativos y reglamentarios aplicables, así como de las mejores prácticas nacionales e internacionales en seguridad de la información.

Acceso a la Información y Control de Usuarios.

- El acceso a los sistemas y la información se basará en el principio de Mínimo Privilegio (Solo el necesario para la función del cargo).
- Se exigirá el uso de contraseñas robustas, cambiadas periódicamente, y se prohibirá su divulgación o uso compartido.
- Se implementarán mecanismos de autenticación segura.

Protección contra Software Malicioso y Malware (Antivirus).

- Todos los dispositivos de IMVIYUMBO deben contar con software de protección antivirus/antimalware debidamente actualizado.
- Se prohíbe la instalación de software no autorizado en equipos de la entidad.
- Se debe tener especial precaución con archivos adjuntos y enlaces de correos electrónicos de origen desconocido o sospechoso (phishing).

Uso aceptable de Activos y Equipos.

- Los recursos tecnológicos de IMVIYUMBO (equipos, software, internet, correo electrónico) son prioritariamente para uso laboral y profesional.
- Se prohíbe el acceso a contenido ilegal, inapropiado o que comprometa la reputación de la entidad.

Seguridad en redes y Telecomunicaciones.

- Se establecerán controles para segregar las redes y proteger los perímetros.
- Se prohíbe la conexión de dispositivos personales a la red institucional sin autorización previa.

Gestión de Incidentes de Seguridad Digital.

- Se establecerá un Procedimiento para la detección, reporte, escalamiento, gestión y resolución de incidentes de seguridad digital.
- Todo evento o incidente de seguridad debe ser reportado inmediatamente al personal de apoyo de gestión TIC.

Formación

- IMVIYUMBO promoverá capacitaciones al personal adscrito a la entidad de formación y sensibilización en seguridad digital.
- Se divulgará la política por todos los canales de comunicación interna para asegurar su conocimiento y apropiación.

Cumplimiento y consecuencias.

- El cumplimiento de esta política es obligatorio para todas las personas dentro de su alcance.
- Esta política será revisada y actualizada periódicamente, o cuando se presenten cambios significativos en el entorno tecnológico o regulatorio de la organización.

LINEAMIENTOS Y DIRECTRICES.

A continuación, se establecen los principios y las reglas básicas para la protección de la información:

Gestión de la Información

- ✓ Clasificación de la Información: Toda la información del Instituto debe ser clasificada según su sensibilidad (Pública, interna, confidencial, etc.) para determinar el nivel de protección requerido.

- ✓ Protección de Datos Personales: Se dará estricto cumplimiento a la política de protección de datos personales de la entidad, garantizando que el tratamiento de esta información se realice conforme a la ley.

- ✓ Manejo de la Información: La información confidencial no debe ser divulgada, modificada o destruida sin la debida autorización.

- ✓ Copias de Respaldo: Se realizarán copias de seguridad periódicas de la información para garantizar la disponibilidad en caso de incidentes.

Control de Acceso

- ✓ Identificación y Autenticación: Se exigirá el uso de nombres de usuario y contraseñas seguras para acceder a los sistemas y la información.

- ✓ Control de Acceso Físico: Se implementarán controles de acceso a las instalaciones donde se procesa y almacena la información sensible.

Uso de Recursos Tecnológicos

- ✓ Uso Aceptable: Los equipos y sistemas de IMVIYUMBO deben usarse para fines laborales. Se prohíbe el uso de software sin licencia o la descarga de contenido malicioso.

- ✓ Correo Electrónico: Se prohíbe el uso del correo institucional para fines personales o ilícitos. Se debe tener precaución con correos electrónicos sospechosos.

- ✓ Internet y Redes Sociales: Se debe hacer uso responsable y ético de internet. Se prohíbe el uso de las redes sociales para divulgar información confidencial o sensible de la entidad.

Gestión de Riesgos y Respuesta a Incidentes

- ✓ Identificación de Riesgos: El proceso de gestión TI, en coordinación con los demás procesos, realizará evaluaciones periódicas de riesgos de seguridad digital.

- ✓ Reporte de Incidentes**:** Todos los incidentes de seguridad (sospechas de virus, pérdida de datos, acceso no autorizado) deben ser reportados de inmediato al área de tecnología.

- ✓ Respuesta a Incidentes: Se contará con un plan de respuesta a incidentes para actuar de manera coordinada ante un evento de seguridad.

ROLES Y RESPONSABILIDADES.

El Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo – IMVIYUMBO define los roles y responsabilidades necesarios para la implementación del Sistema de Gestión y Seguridad de la Información, así como para el cumplimiento de los lineamientos de seguridad establecidos en la presente política y en los demás documentos que lo conforman, los cuales se describen a continuación:

INSTANCIA - PROCESO	RESPONSABILIDADES
Gestión Gerencial	Es la máxima responsable de aprobar y proveer los recursos económicos, humanos y de formación necesarios para la implementación, mantenimiento y mejora continua de esta política.
Gestión TI	Liderar la implementación y monitoreo de la Política de Seguridad Digital.
Gestión del Talento Humano	Controlar y salvaguardar la información de datos personales del personal de planta en concordancia con la normatividad vigente.
Gestión de Control Interno	Definir y aplicar mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento en la implementación de las medidas de seguridad.
Gestión contable y Financiera	Controlar y salvaguardar la información de los datos contables de la entidad mediante el

	aplicativo ASCII, de conformidad con los lineamientos en seguridad digital.
Oficina Asesora de Planeacion y Comité Institucional de Gestión y Desempeño	Orientar la implementación de la Política de Seguridad Digital, conforme a lo establecido en el Modelo Integrado de Planeación y Gestión (MIPG)
Las demás áreas y procesos	Ser corresponsables de la implementación de la política en el ámbito de su competencia, ejecutando las acciones de prevención y mitigación de riesgos, y aplicando buenas prácticas en el tratamiento de los datos y la información de la entidad.

IMPLEMENTACIÓN

Anexo. Plan de Acción Anual de la política de seguridad digital.

RUTA DE APROBACIÓN VERSIÓN 2					
Elaboró		**Revisó**		**Aprobó**	
Nombre	Jhon Pino	Nombre	Evelyn Loaiza Gómez	Comité Institucional de Gestión y Desempeño	
Cargo	Contratista de Apoyo Proceso de Gestión TI.	Cargo	Jefe Oficina Asesora de Planeación	Fecha	Acta de Reunión No 110-02-06-06 23/09/2025

Control de Cambios.

Versión	Fecha (dd/mm/aa)	Aprobado por:	Descripción de la actualización
1	19/07/2022	Uriel Urbano Urbano (Gerente General)	Creación del Documento.
2	23/09/2025	Comité Institucional de Gestión y Desempeño	Actualización de la estructura del documento y elaboración del Plan de Acción para la implementación de la política.