CONTENIDO

INTRODUCCIÓN

En cumplimiento de la Política de Gobierno Digital, la Política de Seguridad y Privacidad de la Información, así como del Modelo de Seguridad y Privacidad de la Información (MSPI) definido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), el Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo - IMVIYUMBO asume el compromiso de seguir los lineamientos establecidos para la implementación de estrategias de seguridad de la información y seguridad digital en las entidades públicas. Esto se llevará a cabo a través de la ejecución de las políticas de Gobierno Digital y Seguridad Digital, cuyo objetivo es garantizar la protección, confidencialidad, integridad y disponibilidad de la información gestionada por la entidad.

Con base en lo anterior, IMVIYUMBO presenta el Plan de Seguridad y Privacidad de la Información para la vigencia 2026, cuyo propósito es fortalecer las medidas de seguridad en el manejo de los datos, garantizando su protección frente a riesgos y amenazas, y asegurando el cumplimiento de las normativas en materia de privacidad y seguridad de la información. De esta manera, IMVIYUMBO reafirma su compromiso con la transparencia y la mejora continua en la gestión de la información pública.

OBJETIVO

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información tiene como objetivo establecer las acciones necesarias para identificar, analizar, priorizar y tratar los riesgos que puedan afectar los activos de información del Instituto Municipal de Reforma Urbana y Vivienda de Interés Social de Yumbo – IMVIYUMBO.

Este plan busca garantizar la protección de la confidencialidad, integridad, disponibilidad y privacidad de la información mediante la implementación de controles adecuados, el cumplimiento de la normativa vigente y la adopción de buenas prácticas de seguridad digital, asegurando así la continuidad operativa, la confianza institucional y la adecuada prestación de los servicios a la ciudadanía.

ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aplica a todos los procesos, áreas, dependencias, sistemas de información, infraestructura tecnológica y activos de información del Instituto Municipal de Reforma Urbana y Vivienda de Interés Social de Yumbo – IMVIYUMBO.

El alcance comprende:

- ✓ Todos los datos institucionales, incluyendo información pública, reservada, confidencial, sensible y datos personales tratados por la entidad.
- ✓ Los activos de información físicos y digitales, tales como documentos, bases de datos, aplicativos, servidores, equipos de cómputo, redes, plataformas tecnológicas y medios de almacenamiento.
- ✓ Los sistemas, aplicaciones y servicios tecnológicos, tanto internos como aquellos administrados por terceros o proveedores que procesen información institucional.
- ✓ Los funcionarios, contratistas y terceros, que acceden, administran, procesan o custodian información institucional en el ejercicio de sus funciones.

- ✓ Los controles de seguridad, procesos y procedimientos institucionales, incluidos los relacionados con gestión del riesgo, continuidad del negocio, protección de datos personales y seguridad digital.

- ✓ Todos los entornos tecnológicos de la entidad, tanto físicos como virtuales, así como los componentes asociados a comunicaciones, seguridad perimetral y servicios críticos.

MARCO NORMATIVO

Categoría	Norma / Estándar	Descripción / Alcance
Nacional	Constitución Política de Colombia (1991)	Art. 15 y 20: derechos a la intimidad, protección de datos personales y acceso a la información.
Nacional	Ley 1581 de 2012	Régimen General de Protección de Datos Personales.
Nacional	Decreto 1377 de 2013	Reglamentación parcial de la Ley 1581; lineamientos sobre autorizaciones y tratamiento de datos.
Nacional	Ley 1266 de 2008	Régimen de Habeas Data financiero e información crediticia.
Nacional	Ley 1273 de 2009	Creación de delitos informáticos y protección de datos y sistemas informáticos.
Nacional	Ley 594 de 2000 (Ley General de Archivos)	Gestión documental, conservación y administración de documentos públicos.
Nacional	Ley 1712 de 2014	Transparencia y acceso a la información pública; requisitos de integridad, disponibilidad y publicación.
Nacional	Decreto 1083 de 2015	Disposiciones de función pública relacionadas con seguridad, control

		interno y administración de la información.
Nacional	Política de Gobierno Digital (Decreto 1008 de 2018 y actualizaciones)	Lineamientos en seguridad digital, privacidad, arquitectura TI y gestión de riesgos.
Nacional	Modelo Integrado de Planeación y Gestión (MIPG)	Enfoque institucional para la gestión del riesgo, control interno y mejora continua.
Nacional	Circulares y guías de la SIC	Lineamientos interpretativos y técnicos para la correcta protección de datos personales.
Internacional	ISO/IEC 27002:2022	Buenas prácticas y controles de seguridad de la información.

TÉRMINOS Y DEFINICIONES

- ✓ **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización (ISO/IEC 27000).

- ✓ **Activo de Información:** Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de la entidad. (CONPES 3854 de 20116).

- ✓ **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

- ✓ **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

- ✓ **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales

(software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- ✓ **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.

- ✓ **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- ✓ **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización (ISO/IEC 27000).

- ✓ **Controles:** Medida que permite reducir o mitigar un riesgo.

- ✓ **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de la entidad, es pública o privada que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

- ✓ **Incidente de Seguridad de la Información:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (GTC-ISO/IEC27035, 2012).

- ✓ **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- ✓ **Información Publica Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento

de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6), Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008., Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

- ✓ **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.
- ✓ **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
- ✓ **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
- ✓ **Sistema de Información:** Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información.
- ✓ **Tecnología de la Información:** Se refiere al hardware y software operado por la entidad.

DESARROLLO DEL PLAN

El Plan de Seguridad y Privacidad de la Información de IMVIYUMBO se fundamenta en el Modelo de Seguridad y Privacidad de la Información propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, el cual recoge las mejores prácticas para establecer los requisitos necesarios en diagnóstico, planificación, implementación, gestión y mejora continua. Este enfoque se adapta específicamente a las necesidades y objetivos de IMVIYUMBO, teniendo en cuenta tanto los requisitos de seguridad de la información como la estructura organizacional y los procesos internos de la entidad.

PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD DE PRIVACIDAD DE LA INFORMACIÓN MSPI

Desde el Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo - IMVIYUMBO, se ha estructurado un plan de trabajo orientado a fortalecer el Modelo de Seguridad y Privacidad de la Información de la entidad, como herramienta fundamental para garantizar el cumplimiento de los lineamientos normativos relacionados con la seguridad y privacidad de la información. Este plan tiene como objetivo principal consolidar las acciones necesarias para asegurar la protección adecuada de los activos de información de la entidad.

A continuación, se presenta el plan, el cual detalla las actividades, tareas, responsables y las fechas de programación tentativas para su ejecución durante la vigencia 2026.

PLAN DE TRABAJO VIGENCIA 2026

Actividad	Tarea / Descripción Mejorada	Responsable	Programación (2026)
Diagnóstico de la gestión de seguridad de la información	Elaborar el diagnóstico de la situación actual de la gestión de seguridad de la información, identificando brechas, necesidades, controles existentes y oportunidades de mejora.	Oficina Asesora de Planeación – Proceso Gestión TI	Marzo 2026
Levantamiento de Activos de Información	Realizar el inventario y registro detallado de los activos de información (datos, aplicaciones, sistemas, infraestructura y recursos tecnológicos). Identificar su criticidad, propietarios y dependencias para fortalecer su gestión y protección.	Oficina Asesora de Planeación – Proceso Gestión TI – Líderes de Proceso	Marzo 2026
Jornadas de capacitación en seguridad y privacidad	Planificar, coordinar y ejecutar jornadas de sensibilización y capacitación dirigidas a funcionarios y contratistas, enfocadas en buenas prácticas de seguridad digital, protección de datos personales y prevención de incidentes.	Oficina Asesora de Planeación – Proceso Gestión TI	Junio 2026 – Noviembre 2026

Establecimiento de indicadores de gestión de seguridad	Definir e implementar indicadores que permitan medir la eficacia, eficiencia y nivel de cumplimiento de los controles del modelo de seguridad y privacidad de la información.	Oficina Asesora de Planeación – Proceso Gestión TI	Noviembre 2026
Protección de la Información – Copias de Seguridad	Ejecutar y verificar la realización de copias de seguridad semanales de las bases de datos institucionales, asegurando su integridad, disponibilidad y correcta restauración.	Proceso Gestión TI	Permanente
Seguridad Perimetral y Antivirus	Configurar, monitorear y hacer seguimiento continuo a la seguridad perimetral, firewall, sistema de detección de intrusiones y consola antivirus, garantizando la protección frente a amenazas internas y externas.	Proceso Gestión TI	Permanente
Mantenimiento de infraestructura tecnológica	Ejecutar el mantenimiento preventivo y correctivo de equipos de cómputo, servidores, redes y demás elementos tecnológicos, garantizando su operación eficiente y segura.	Proceso Gestión TI	Junio 2026 – Diciembre 2026

CUMPLIMIENTO DE LA IMPLEMENTACIÓN

El cumplimiento de la implementación del Plan de Trabajo para la vigencia 2026 se evaluará mediante el seguimiento periódico a las actividades, tareas e indicadores definidos para cada fase del proceso. Este cumplimiento será verificado por el Proceso de Gestión TI y la Oficina Asesora de Planeación, quienes garantizarán que las acciones programadas se ejecuten conforme a los tiempos establecidos, los lineamientos institucionales y los requisitos normativos vigentes en materia de seguridad y privacidad de la información.

1. Las actividades y tareas planificadas se ejecuten en los plazos establecidos, evidenciando su desarrollo mediante actas, informes, registros, inventarios, reportes técnicos o documentos de soporte.

2. Los controles y acciones definidas hayan sido aplicados de manera efectiva, contribuyendo a la mitigación de los riesgos identificados en el diagnóstico y fortaleciendo la gestión institucional de seguridad digital.

3. Los indicadores definidos permitan medir el avance, la eficacia y la eficiencia de las acciones implementadas, proporcionando información clara y verificable para la toma de decisiones.

4. Los responsables de cada actividad generen y entreguen la evidencia correspondiente, la cual será revisada y archivada conforme a las políticas institucionales de gestión documental.

5. Se realicen actividades de verificación y seguimiento, con el fin de evaluar los resultados, detectar desviaciones y establecer acciones correctivas o de mejora continua.

6. Los resultados se reporten a los niveles directivos correspondientes, fortaleciendo la transparencia, el control interno y la alineación con las políticas de Gobierno Digital, MIPG y seguridad de la información.

MEDICIÓN

Monitoreo de Cumplimiento del Plan de Seguridad y Privacidad de la Información

Para garantizar el éxito en la implementación y cumplimiento del Plan de Seguridad y Privacidad de la Información, es esencial llevar a cabo un seguimiento continuo y riguroso de las actividades. Para ello, se ha definido el siguiente indicador de eficacia:

Indicador de Cumplimiento de Requerimientos de TI:

Índice de Cumplimiento: (No de requerimientos resueltos (x)/No de requerimientos solicitados (Y)) *100

Para el cumplimiento del plan de Seguridad y Privacidad de la Información de la entidad es preciso monitorear y controlar las actividades por lo cual se ha establecido el siguiente indicador de eficacia:

Periodicidad: Este indicador será medido y reportado Cuatrimestralmente a la Oficina Asesora de Planeación para asegurar el seguimiento oportuno de los avances y la toma de decisiones informada.

Este indicador permitirá evaluar la eficiencia y efectividad en la resolución de los requerimientos tecnológicos relacionados con la seguridad y privacidad de la

información, permitiendo ajustes cuando sea necesario para alcanzar los objetivos del plan.

RUTA DE APROBACIÓN VERSIÓN 7					
Elaboró		**Revisó**		**Aprobó**	
Nombre	John Alexander Pino	Nombre	Evelyn Loaiza Gómez	Comité Institucional de Gestión y Desempeño	
Cargo	Personal de Apoyo	Cargo	Jefe Oficina Asesora de Planeación	Fecha	Acta No 110-02-06-01 22/01/2026

Control de Cambios:

Versión	Fecha (dd/mm/aa)	Descripción de la actualización
1	06/07/2018	Creación del Documento.
2	29/01/2021	Actualización periodo 2021.
3	17/01/2022	Actualización periodo 2022.
4	20/01/2023	Actualización periodo 2023.
5	24/01/2024	Actualización periodo 2024.
6	24/01/2024	Actualización periodo 2025.
7	22/01/2026	Actualización periodo 2026.