INTRODUCCIÓN

El Modelo Integrado de Planeación y Gestión MIPG es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio, según dispone el Decreto1499 de 2017.

Mejorar la capacidad del Estado para cumplirle a la ciudadanía, incrementando la confianza de la ciudadanía en sus entidades y en los servidores públicos, logrando el compromiso del servidor publico, mayor presencia en el territorio y mejor aprovechamiento y difusión de información confiable y oportuna es una de los objetivos de la puesta en marcha del Modelo Integrado de Planeación y Gestión MIPG.

La presente Política de Seguridad y Privacidad de la Información del Instituto corresponde a un acto administrativo general que representa la posición del Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo - IMVIYUMBO, con respecto a los criterios formales para la protección de los activos de su información y la que utiliza para sus fines misionales. Esto se realiza en el marco de lo que compete a las actuaciones de los Servidores del Estado, funcionarios, contratistas, terceros relacionados con la entidad, los procesos de la misma, las tecnologías de información que son usados en ésta; en tanto que soportan los procesos y los procedimientos del Sistema Integrado de Gestión Institucional de la Entidad y apoyan la implementación específica del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de las políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para garantizar que se materialice una gestión administrativa en la que se priorice la seguridad de la información que se utiliza y se comunica desde este ente descentralizado territorial.

JUSTIFICACIÓN

El Instituto, con el propósito de salvaguar la información de la entidad en todos sus aspectos y en consecuencia garantizando la seguridad de los datos y el cumplimiento de las normas legales; ha realizado un Plan de Seguridad y Privacidad de su información, con el ánimo de evitar pérdidas, sustracciones indebidas, accesos no autorizados y duplicidad innecesaria de su información y de aquella que use en razón de sus objetivos misionales. De la misma manera, El Instituto promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios internos, los externos y demás actores que con él se relacionan.

En el marco de esta política, La seguridad de la información se entiende como la preservación de las siguientes características:

- Confidencialidad: Sin perjuicio del principio constitucional de la publicidad, se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- Integridad: Se salvaguarda la idoneidad, la exactitud y el manejo integral de la totalidad de la información y los métodos utilizados para su procesamiento.
- Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, en el proceso de implementación progresiva de esta política Institucional en las entidades públicas del municipio de Yumbo, deben de considerarse los conceptos de:

1. Protección a la duplicación: Permanentemente los responsables de una transacción. Gestionarán que sólo se realice una vez, a menos que se especifique lo contrario. Es necesario limitar que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
2. No repudio: En aplicación al principio constitucional de buena fe, el miembro de una entidad que haya enviado o recibido información no podrá alegar ante terceros que no la envió o recibió.

3. Legalidad: Cada actuación relacionada con el uso de información se sujetará integralmente al cumplimiento de las disposiciones constitucionales, leyes, normas inferiores, reglamentaciones o disposiciones a las que está sujeto el Organismo.
4. Confiabilidad de la Información: La información generada será la adecuada, necesaria, verificada y oportuna para sustentar la toma de decisiones y la ejecución de las misiones y funciones institucionales.

OBJETIVO

Definir las políticas de seguridad digital que se deben seguir por parte de los colaboradores del Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo – IMVIYUMBO, con el fin de preservar la disponibilidad, integridad y confidencialidad de la información.

OBJETIVOS ESPECIFICOS

- Salvaguardar los activos tecnológicos y custodiar la información producida en IMVIYUMBO.
- Promover la cultura de la seguridad de la información a los servidores públicos y contratistas.
- Capacitar al personal de IMVIYUMBO en buenas practicas digitales.

ALCANCE

Las políticas definidas aplican para todos los Servidores Públicos y colaboradores del Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo - IMVIYUMBO que requieran utilizar Internet, Correo electrónico y acceder a los sistemas de información.

CONCEPTOS BÁSICOS

- **Activo de Información**: Es todo aquello que en la entidad es considerado importante o de alta validez para la misma ya que puede contener información

importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.

- **Amenaza**: Es una circunstancia que tiene el potencial de causar un daño o una perdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.
- **Confidencialidad**: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Copias de respaldo**: Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su perdida.
- **Dato**: Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **Disponibilidad**: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Gestión de riesgos de seguridad digital**: es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.
- **Integridad**: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Información**: Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

NORMATIVIDAD

Ley 1341 de 2009 Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

LEY 1273 DE 2009 “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 1474 de 2011 Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión publica

LEY 1712 DE 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Publica Nacional y se dictan otras disposiciones.

Decreto 1078 de 2015 Art. 2.2.9.1.2.2 contemplo los instrumentos para implementar la Estrategia de Gobierno en Línea, dentro de los cuales se exige la elaboración por parte de cada entidad un Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI, un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información.

LINEAMIENTOS PARA MEDIOS REMOVIBLES

Son medios removibles todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores, para lo cual se establecen los siguientes lineamientos.

- El servicio de acceso a Internet, Intranet, Sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de computo son propiedad de IMVIYUMBO y deben ser usados únicamente por entidad.
- El manejo, configuración, y actualización de la pagina institucional es exclusivamente de IMVIYUMBO.
- Los usuarios deben tratar los mensajes de correo electrónico, chat y archivos adjuntos como información de propiedad de IMVIYUMBO.
- Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

- Cuando un funcionario que tiene asignada una cuenta de correo de la entidad, deberá entregar los usuarios y password asignados, de igual manera dicha información debe entregarse cuando exista un proceso de empalme.

POLITICA DE TRATAMIENTO DE DATOS

Los datos personales que los ciudadanos, usuarios, servidores públicos, proveedores que suministren al Instituto, en cualquiera de sus procesos, serán utilizados para la prestación del servicio solicitado y serán incorporados en una base de datos cuya responsabilidad y manejo está a cargo de IMVIYUMBO. Los datos personales suministrados serán administrados de forma confidencial y con la finalidad de brindar los servicios y el soporte requerido por el usuario, con las debidas garantías constitucionales, legales y demás normas aplicables a la protección de datos personales.

IMVIYUMBO, transferirá la información a un tercero únicamente si está obligado a hacerlo por orden de autoridad administrativa o judicial.

IMVIYUMBO, se abstiene de ceder, vender o compartir los datos de carácter personal recolectados, sin la expresa autorización del usuario.

IMVIYUMBO, no responderá en ningún caso y bajo ninguna circunstancia, por los ataques o incidentes contra la seguridad de su sitio web o contra sus sistemas de información; o por cualquier exposición o acceso no autorizado, fraudulento o ilícito a su sitio web y que afecten la confidencialidad, integridad o autenticidad de la información publicada o asociada con los contenidos y servicios que se ofrecen en el.

El Tratamiento de los datos se realizará para:

La vinculación, desempeño de funciones o prestación de servicios, retiro o terminación. Para seguridad de las personas, los bienes e instalaciones de la Institución. Para los fines relacionados con el desarrollo el proceso de gestión contractual de productos o servicios que la entidad requiera para su funcionamiento de acuerdo a la normatividad vigente.

Acuerdo de Confidencialidad

Implica que la información conocida por todo funcionario, contratista y/o tercero, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización.

Seguridad de Computadores y Portátiles

Para lograr un alto rendimiento y salvaguarda de computadores y portátiles, la administración municipal ha definido los siguientes parámetros.

- Los computadores de mesa, portátiles, y cualquier activo de tecnología de información, podrán salir de las instalaciones únicamente con la aprobación del Jefe del área.
- El equipo de computo asignado, deberá ser para uso exclusivo de las funciones de la Institución.
- Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del computador.
- Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previniendo así la perdida involuntaria de información, derivada del proceso de reparación.
- Los equipos de IMVIYUMBO solo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.
- Debe respetarse y no modificar la configuración de hardware y software establecida por la Institución.
- Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario.
- El personal que utiliza un computador portátil que contenga información confidencial de la institución, no debe dejarlo desatendido, sobre todo cuando esté de viaje.
- Se prohíben que los equipos estén en contacto con piso, el usuario debe disponerlo (computador y/o Portátil) sobre el escritorio.
- Los recursos de IMVIYUMBO, utilizados para el procesamiento de la información deben ser ubicados en sitios estratégicos, que faciliten el trabajo compartido, el trabajo colaborativo, la optimización de recursos.

GENERALIDADES

El Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo – IMVIYUMBO ha diseñado este instrumento concertadamente con sus diferentes actores involucrados el presente plan, con el propósito de garantizar el direccionamiento estratégico de la Entidad y establece la compatibilidad de la política y de los objetivos de seguridad de la información.

Las actividades del presente plan se realizarán en particular en lo que corresponde a los siguientes componentes:

1. Monitorear, controlar o mitigar los riesgos en el uso de información de la entidad.
2. Cumplir con los principios de seguridad de la información.
3. Cumplir con los principios de la debida función administrativa.
4. Mantener la confianza de los sujetos intervinientes en los diferentes procesos, en particular de los servidores del estado, los funcionarios, los contratistas y terceros involucrados.
5. Apoyar las políticas de innovación tecnológica.
6. Implementar el sistema de gestión de seguridad de la información.
7. Proteger los activos de información.
8. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
9. Fortalecer la cultura de seguridad de la información en los Servidores del estado, los funcionarios y los demás clientes internos y externos del Instituto como órgano descentralizado municipal.
10. Garantizar la continuidad del servicio público de acceso a la información de la entidad frente a eventuales incidentes.
11. Incorporar progresivamente este plan, sus programas y sus actividades en el marco de la política municipal de Privacidad de la información pública, en los términos del modelo de gestión pública municipal correspondiente.

A continuación, se establecen las políticas que soportan el plan de seguridad y privacidad de la información del Instituto; razón por la cual de manera formal quienes hacen parte del Instituto están obligados a:

a) Amparar en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza institucional de entidad pública territorial descentralizada del orden municipal.

b) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los involucrados en su uso, disposición, conservación y difusión.
c) El Instituto protege la información generada, procesada o resguardada por los procesos y los diferentes procedimientos de la entidad y los activos de información que hacen parte de los mismos.
d) El Instituto protege la información creada, procesada, transmitida o resguardada por sus procesos de la entidad, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
e) El Instituto protege su información de las amenazas originadas por parte del personal que accede a ella o la utiliza de manera indirecta.
f) El Instituto protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos diferentes procesos, especialmente aquellos de nivel crítico.
g) El Instituto controla la operación de sus procesos de la entidad garantizando la seguridad de los recursos tecnológicos y las redes de datos.
h) El Instituto implementa controles de acceso a la información, sistemas y recursos de red.
i) El Instituto garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
j) El Instituto garantiza a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
k) El Instituto garantiza la disponibilidad de sus procesos de la entidad y la continuidad de su operación basada en el impacto que pueden generar los eventos.
l) El Instituto garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la Política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

Roles y Responsabilidades:

Es responsabilidad de Planeación del Instituto la implementación, aplicación, seguimiento y autorizaciones de la Política; así como de definir los mecanismos y todas las medidas necesarias por parte de del Plan de Seguridad y Privacidad de la información en las diferentes áreas y procesos de la entidad, además garantiza el apoyo y el uso de la Política de Seguridad de la Información como parte de su herramienta de gestión, la cual debe ser aplicada de forma obligatoria por todos los funcionarios para el cumplimiento de los objetivos.

FIN DEL DOCUMENTO

Elaboró:	Revisó:	Aprobó:
MILTON MARINO PULIDO DAVILA	JOSÉ ARLES NARVÁEZ ALVAREZ	URIEL URBANO URBANO
CARGO: PROFESIONAL EN INGENIERIA DE SISTEMAS (CONTRATISTA)	CARGO: DIRECTOR ADMIISTRATIVO Y FINANCIERO	CARGO: GERENTE
Firma:	Firma:	Firma:

ANEXO

A). Control de Cambios

Versión	Fecha (dd/mm/aa)	Aprobado por:	Descripción de la actualización
1	01/08/2022	Uriel Urbano Urbano (Gerente)	Creación del Documento.