INSTITUTO MUNICIPAL DE REFORMA URBANA Y DE VIVIENDA DE INTERES SOCIAL DE YUMBO - IMVIYUMBO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2024

Gestión de Planeación
24-01-2024

Contenido

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información está basado en los lineamientos presentados en la guía de seguridad y privacidad de información del Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.

Este plan se encuentra articulado con las políticas contenidas en el Modelo Integrado de Planeación y Gestión MIPG: Transparencia, Acceso a la Información Pública y Lucha contra la Corrupción, Gobierno Digital y Seguridad Digital.

IMVIYUMBO es consciente que la protección y aseguramiento de su información es fundamental para garantizar su debida gestión administrativa y operativa, razón por la cual debe establecer un marco normativo de Seguridad de la Información que contemple políticas, límites, responsabilidades y obligaciones frente a la seguridad y privacidad de la información de la entidad.

En el presente documento se desarrolló el Plan de seguridad y privacidad de la información para el Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo – IMVIYUMBO, el cual tomará como referencia el Modelo de Seguridad y Privacidad de la Información –MSPI, de la estrategia de Gobierno en Línea, esta proporciona un marco metodológico basado en buenas prácticas para llevar a cabo la implementación de un modelo de Gestión de Seguridad y Privacidad de la información en cualquier tipo de organización, lo cual, permite garantizar su efectiva implementación y asegurar su debida permanecía y evolución en el tiempo.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

JUSTIFICACIÓN

El Instituto de Reforma Urbana y Vivienda de Interés social de Yumbo - IMVIYUMBO con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la Información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados, 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, externos y demás actores que con él se relacionan.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

ALCANCE

Este Plan de Seguridad y Privacidad de la Información y su Política, son aplicables a todos los funcionarios del Instituto de Reforma Urbana y Vivienda de Interés social de Yumbo IMVIYUMBO, a sus recursos, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la entidad y terceras partes, que usen activos de información que sean propiedad de la entidad. El plan está formulado para que se ejecute durante la vigencia 2024 tiempo necesario para lograr la adopción del MSPI y garantizar su continuidad.

Comprende para cada Líder de proceso de la Entidad, mantener una adecuada gestión de riesgos de seguridad y privacidad de la información y su seguimiento, y se desarrolla al abordar los pasos metodológicos, lineamientos, guías, herramientas y mejores prácticas para el cubrimiento de brechas de seguridad y privacidad de la información.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

OBJETIVOS

OBJETIVO GENERAL

- Desarrollar un plan de seguridad y privacidad que permita minimizar los riesgos de pérdida de activos de la información en IMVIYUMBO para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno en línea.

OBJETIVOS ESPECÍFICOS

- Proteger los activos de información del Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo - Imviyumbo con base en los criterios de confidencialidad, integridad y disponibilidad.

- Sensibilizar a los servidores públicos y contratistas de la entidad acerca del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, promoviendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información críticos de Imviyumbo.

- Realizar un diagnóstico de los activos de información para minimizar los riesgos.

- Tener políticas y prácticas de seguridad que logren guiar el comportamiento de los funcionarios y contratistas de la Institución, sobre la información generada y procesada en la entidad.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

TÉRMINOS Y DEFINICIONES

Activo: Es un recurso que tiene un valor específico para la entidad y debe ser protegido.

Análisis de riesgo: Uso metódico de la información para identificar fuentes y para evaluar el riesgo.

Antivirus: Software diseñado para la detección, prevención y eliminación de programas y archivos maliciosos o dañinos, en equipos de cómputo y dispositivos.

Auditabilidad: Permite que todos los eventos de un sistema deben de ser registrados, con evidencia probable para su control posterior, por quien hace parte del sistema o por ente auditor externo, en el marco de un plan anual de auditorías o seguimiento previamente comunicado.

Ciberseguridad: Procedimientos y herramientas que se implementan para proteger la información que se genera a través de equipos de cómputo, servidores, dispositivos móviles, redes y sistemas electrónicos.

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.

Confidencialidad: Propiedad de la información por la que se garantiza que está accesible únicamente a personal autorizado.

Control de acceso: Significa garantizar que el acceso a los activos esté autorizado y restringido, según los requisitos comerciales y de seguridad.

Criptografía: El procedimiento de transmitir datos y mensajes cifrados.

Disponibilidad: El proceso de asegurar que la información sea accesible para usuarios autorizados cuando ellos lo requieran.

Evento de seguridad: Una situación previamente desconocida que pueda ser relevante para la seguridad.

Encriptación: Codificación de los datos para evitar que los usuarios no autorizados los modifiquen. Sólo los usuarios con acceso a una contraseña pueden descifrar y utilizar los datos.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

Hacking Ético: Actividades encaminadas a realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas para evitar daños y alterar los datos.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Ingeniería Social: Método utilizado por los atacantes para engañar a los usuarios, para que realicen una acción, que normalmente producirá consecuencias negativas, como perdida de la información o descarga de virus.

Integridad: Propiedad que busca mantener los datos libres de modificaciones no autorizadas y asegurar que los datos del sistema no hayan sido alterados, ni cancelados por personas, entidades no autorizadas y que el contenido de los mensajes recibidos es el correcto.

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

IMVIYUMBO: Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo.

MSPI: (Modelo de Seguridad y Privacidad de la información) Actividades, acciones y procesos para proteger el acceso, uso y divulgación del acceso a la información.

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.

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.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

SGSI: (Sistema de Gestión de Seguridad de la Información). Procesos y procedimientos para gestionar el acceso a la información encaminados a buscar confidencialidad, integridad y disponibilidad de los activos y minimizando los riesgos.

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.

Tratamiento del riesgo: Proceso de análisis e implementación de acciones de mejorar que permitan gestionar el riesgo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotado por una o más amenazas.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

MARCO NORMATIVO

Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23/1982 y se modifica la Ley 29/1944 Ley 527/1999. Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación.

Ley 594 de 2000. Se expide la Ley General de Archivos.

Ley 1266 de 2008. Se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios, y la proveniente de terceros países.

Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo.

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

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 TICS.

Ley 1474 de 2011. Orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción.

Ley 1581 de 2012. Disposiciones generales para la protección de datos personales.

Ley 1712 de 2014. Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.

Ley 1915 de 2018. Por la cual se modifica la Ley 23/1982.

Ley 1978 de 2019. Se moderniza el sector de las TIC. Dec. 2609/2012. Por el cual se reglamenta el Título V de la Ley 594/2000, parcialmente los artículos 58 y 59 de la Ley 1437/2011

Decreto 0884 del 2012. Reglamenta parcialmente la Ley 1221/2008.

Decreto 1377 de 2013. Reglamenta parcialmente la Ley 1581/2012.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

Decreto 886 de 2014. Reglamenta el Registro Nacional de Bases de Datos.

Decreto 103 de 2015. Reglamenta parcialmente la Ley 1712/2014.

Decreto 1078 de 2015. Expide el Decreto Único Reglamentario del Sector de las TIC.

Decreto 728 de 2017. Adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078/2015, para fortalecer el modelo de Gobierno Digital.

Decreto 1499 de 2017. Modifica el Dec.1083/2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el art 133 de la Ley 1753/2015.

Decreto 1008 del 2018. 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 Dec.1078/2015, Decreto Único Reglamentario del sector de las TIC.

Decreto 2106 de 2019. Se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.

Decreto 620 de 2020. Por el cual se subroga el título 17 de la parte 2 del libro 2 del Dec.1078/2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437/2011, los literales e), j) y literal a) del parágrafo 2 del art. 45 de la Ley 1753/2015, el numeral 3 del art.147 de la Ley 1955/2019, y el art.9° de Dic. 2106/2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

CONPES 3854 de 2016. Política Nacional de Seguridad Digital.

CONPES 3905 de 2020. Política Nacional de Confianza y Seguridad Digital

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

LINEAMIENTOS ESTRATÉGICOS DE LA INSTITUCIÓN

Con base en el análisis del déficit de vivienda en el Municipio de Yumbo se fijan los lineamientos estratégicos para el período de 2020-2023, quedando así la misión, visión y objetivos Estratégicos para IMVIYUMBO.

- **MISIÓN**
  El Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo IMVIYUMBO es la entidad encargada de promover la oferta de vivienda de interés social y prioritario, mejorar las condiciones básicas de habitabilidad, adelantar los procesos de legalización y titulación de los predios irregulares ubicados en el Municipio y contribuir al desarrollo urbano Municipal, dentro de un marco de saneamiento básico y óptimas condiciones ambientales.

- **VISIÓN**
  El Instituto Municipal de Reforma Urbana y Vivienda de Interés Social de Yumbo – IMVIYUMBO, se consolidará al 2025 como una Institución referente en el sector Vivienda, que contribuye a implementar acciones para generar un hábitat más saludable en la calidad de vida de los habitantes urbanos y rurales del Municipio de Yumbo.

- **POLITICA DE CALIDAD**
  El compromiso del Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo IMVIYUMBO, es satisfacer las necesidades básicas de habitabilidad de la comunidad Yumbeña prestando un servicio con calidad humana oportuna y eficaz, para ello contamos con un talento humano competente y comprometido con el mejoramiento continuo de los Sistemas Integrados de Gestión Institucional - SIGI para a su vez contribuir al Desarrollo Sostenible del Municipio.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

Objetivos de Calidad

- ✓ Mejorar los niveles de satisfacción de los usuarios internos y externos a través de la atención, orientación y asesoría con calidad y calidez humana.
- ✓ Atender oportunamente las necesidades básicas de habitabilidad de la comunidad Yumbeña.
- ✓ Fortalecer la competencia del talento humano del Instituto.
- ✓ Mejorar los Sistemas Integrados de Gestión Institucional – SIGI desde los lineamientos del Modelo Institucional de Planeación y Gestión (MIPG).
- ✓ Lograr el desarrollo sostenible esperado.

- **VALORES**

  Por Valores se entiende aquella forma de ser y de actuar de las personas que son altamente deseables como atributos o cualidades, por cuanto posibilitan la construcción de una convivencia gratificante en el marco de la dignidad humana.

  Cada uno de los valores que se incluyen en el Código de Integridad de IMVIYUMBO, determinan una línea de acción cotidiana para los servidores, de las cuales se definieron los siguientes valores:

  - ✓ **Honestidad:** Actúo siempre con fundamento en la verdad, cumpliendo mis deberes con transparencia, rectitud, y siempre favoreciendo el interés general.
  - ✓ **Respeto:** Reconozco, valoro y trato de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición.
  - ✓ **Compromiso:** Soy consciente de la importancia de mi rol como servidor público y estoy en disposición permanente para comprender y resolver las necesidades de las personas con las que me relaciono en mis labores cotidianas, buscando siempre mejorar su bienestar.
  - ✓ **Diligencia:** Cumplo con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención, prontitud y eficiencia, para así optimizar el uso de los recursos del Estado.
  - ✓ **Justicia:** Actúo con imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

- **OBJETIVOS ESTRATEGICOS INSTITUCIONALES**
  - ✓ Fortalecer administrativamente el sistema de gestión mediante la simplificación de procesos y la optimización de los recursos
  - ✓ Contribuir a la calidad de vida a través de la ejecución de programas de vivienda y hábitat para la población del Municipio de Yumbo
  - ✓ Mejorar el servicio al ciudadano
  - ✓ Mejorar la cultura organizacional y el desempeño del personal

MAPA DE PROCESOS

METODOLOGÍA.

FASES PARA IMPLEMENTAR E INSTRUMENTAR EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

Las fases que se requieren para instrumentar el Modelo son:

- ✓ Fase de Diagnóstico: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

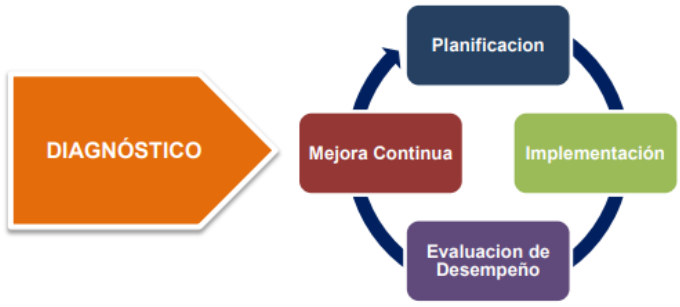
Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

- ✓ Fase Planificación (Planear): En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.

- ✓ Fase Implementación (Hacer): En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.

- ✓ Fase Evaluación de desempeño (Verificar): Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.

- ✓ Fase Mejora Continua (Actuar): Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.



Ciclo de operación del Modelo de Seguridad y Privacidad de la Información
Fuente: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

FASE DE DIAGNÓSTICO

En esta fase se pretende identificar el estado actual de IMVIYUMBO con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información. Para ello se recomienda utilizar los siguientes instrumentos:

- ✓ Herramienta de diagnóstico.
- ✓ Instructivo para el diligenciamiento de la herramienta.
- ✓ Guía No 1 - Metodología de Pruebas de Efectividad.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

Etapas previas a la implementación

Actividades	Instrumento	Resultado	Responsable
1. Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Herramienta de evaluación brindada por el MINTIC.	Diligenciamiento de la herramienta.	Proceso Gestión de Tecnologías.
2. Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad. Utilizando la Herramienta de Diagnostico brindada por el MINTIC.	Utilizando la Herramienta de Diagnostico brindada por el MINTIC.	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad	Proceso Gestión de Tecnologías.
3.Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Utilizando la Herramienta de Diagnostico brindada por el MINTIC.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Proceso Gestión de Tecnologías.

Objetivos del diagnóstico.

- ✓ Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Institución.
- ✓ Determinar el nivel de madurez de los controles de seguridad de la información.
- ✓ Identificar el avance de la implementación del ciclo de operación al interior de la Institución.
- ✓ Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- ✓ Identificación del uso de buenas prácticas en ciberseguridad.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

FASE DE PLANIFICACIÓN

IMVIYUMBO, utilizará los resultados obtenidos en la fase de diagnóstico para proceder a elaborar el Plan de Seguridad de la Información.

PLANIFICACIÓN			
Actividades	Instrumento	Resultado	Responsable
1.Crear la Política General de Seguridad y Privacidad de la Información	Guía No 2 – Política General MSPI	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad	Proceso Gestión de Tecnologías.
2.Políticas de seguridad y privacidad de la información	Guía no 2 - Política General MSPI	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.	Proceso Gestión de Tecnologías.
3.Procedimientos de seguridad de la información	Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Proceso Gestión de Tecnologías.
4. Roles y responsabilidades de seguridad y privacidad de la información.	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.	Proceso Gestión de Tecnologías.
5. Integración del MSPI con el Sistema de Gestión documental	Guía No 6 - Gestión Documental	Integración del MSPI, con el sistema de gestión documental de la entidad.	Proceso Gestión de Tecnologías.
6.Identificación, Valoración y tratamiento de riesgo	Guía No 7 - Gestión de Riesgos Guía No 8 - Controles de Seguridad	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos	Proceso Gestión de Tecnologías.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

		revisados y aprobados por la alta Dirección	
7.Plan de Comunicaciones	Guía No 14 - Plan de comunicación, sensibilización y capacitación	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Proceso Gestión de Tecnologías.

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La presente Política pública 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 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.

El Instituto 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.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

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.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

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.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN EL INSTITUTO MUNICIPAL

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.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

- ✓ **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.

Cumplimiento de la Política:

El cumplimiento de la Política de Seguridad y Privacidad de la Información es obligatorio. Si los funcionarios de la entidad o terceros no atienden el contenido integral de este plan, El Instituto comunicará al organismo competente para que adopte las medidas correspondientes.

Generalidades:

El Instituto municipal de Reforma Urbana y Vivienda de Interés Social de Yumbo - IMVIYUMBO, en todas sus areas y procesos cuenta con información, reservada, relevante, privilegiada e importante; es decir que esta información es el principal activo de la entidad para el desarrollo de todas sus actividades por lo que se hace necesario y se debe proteger conforme a los criterios y principios de los sistemas de información, como son integridad, disponibilidad y confidencialidad de la información. De acuerdo a

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

esta Política se divulgan los objetivos y alcances de seguridad de la información de la entidad, que se logran por medio de la aplicación de controles de seguridad, con el fin de mantener y gestionar el riesgo como lo establece la política de riesgos institucional. Este documento tiene el objetivo de garantizar la continuidad de los servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los objetivos institucionales y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad en la entidad.

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.

POLÍTICA PARA LA IDENTIFICACIÓN, CLASIFICACIÓN Y CONTROL DE ACTIVOS DE INFORMACIÓN

El Instituto realizará la supervisión de cada proceso, el cual debe aprobar el inventario de los activos de información que procesa y produce la entidad, estas características del inventario deben establecer la clasificación, valoración, ubicación y acceso de la información, correspondiendo a Gestión de TIC y a Gestión Documental brindar herramientas que permitan la administración del inventario por cada área, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

El Líder del proceso de Gestión de Tecnologías con apoyo del técnico operativo de sistemas tiene la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la entidad.

Pautas para tener en cuenta

a) Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión y la eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la entidad.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

b) La información física y digital de El Instituto debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de conservación, se le debe dar el tratamiento de acuerdo a la disposición final definida por la entidad.
c) Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíen faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada o mal intencionada.
d) Tanto los funcionarios como el personal provisto por terceras partes deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.
e) La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED

El técnico operativo de sistemas de la Entidad, como responsable de las redes de datos y los recursos de red de la entidad, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

Pautas para tener en cuenta:

a) El proceso Gestión de TIC debe asegurar que las redes inalámbricas del Instituto cuenten con métodos de autenticación que evite accesos no autorizados.
b) El proceso Gestión de TIC debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red del Instituto, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

c) Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de la Entidad, deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el acuerdo de Confidencialidad firmado previamente.
d) Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos del Instituto deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

El Instituto establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Entidad. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas establecidas para tal fin.

Pautas para tener en cuenta

a) El proceso Gestión de TIC, debe definir lineamientos para la configuración de contraseñas que aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información del Instituto; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.
b) El proceso Gestión de TIC debe establecer un protocolo que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.
c) El proceso Gestión de TIC debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.
d) Es responsabilidad de los propietarios de los activos de información, definir los perfiles de usuario y autorizar, conjuntamente con el proceso Gestión de TIC, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

e) Los propietarios de los activos de información deben verificar y ratificar anualmente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

POLÍTICA DE CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN Y APLICATIVOS

El Instituto, como propietario de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada. El proceso Gestión de TIC, como responsable de la administración de dichos sistemas de información y aplicativos, propende para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, vela porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

Pautas para tener en cuenta:

a) Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.
b) Los propietarios de los activos de información deben monitorear anualmente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.
c) El proceso Gestión de TIC debe establecer un protocolo para la asignación de accesos a los sistemas y aplicativos de la Entidad.
d) El proceso Gestión de TIC debe establecer el protocolo y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
e) El proceso Gestión de TIC debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

f) Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.
g) Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.
h) Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla.

POLÍTICAS DE SEGURIDAD FÍSICA

El Instituto provee la implantación y vela por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus dependencias. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considera áreas de acceso restringido.

Se debe tener acceso controlado y restringido a donde se encuentra los servidores y el cuarto de comunicaciones. El proceso Gestión de TIC mantiene las normas, controles y registros de acceso a dichas áreas.

Pautas para tener en cuenta:

a) Las solicitudes de acceso al área donde se encuentra el servidor o los centros de cableado deben ser aprobadas por funcionarios que apoyan el proceso Gestión de TIC autorizados; no obstante, los visitantes que sean siempre deberán estar acompañados de un funcionario.
b) El proceso Gestión de TIC debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; previo registro de tal autorización.
c) La Gerencia de la Entidad proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de la Entidad.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

d) La Gerencia de la Entidad debe identificar mejoras a los mecanismos implantados y de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la entidad.
e) Los ingresos y egresos de personal a las instalaciones del Instituto en horarios no laborales deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.
f) Los funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones del Instituto; en caso de pérdida del carné, deben reportarlo a la mayor brevedad posible.
g) Aquellos funcionarios o personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.

POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS TECNOLÓGICOS

El Instituto para evitar la pérdida, sustracción o exposición indebida al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, proveerá oportunamente los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

Elementos a considerar:

a) El proceso Gestión de TIC debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones del Instituto.
b) El proceso Gestión de TIC debe realizar soportes técnicos y velar que se efectúen los mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la entidad.
c) El proceso Gestión de TIC en conjunto con el facilitador del proceso Gestión de Recursos Físicos debe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del área donde se ubica el servidor y otras áreas de procesamiento de información.
d) El proceso Gestión de TIC debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la entidad y configurar dichos equipos acogiendo los estándares generados.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

e) El proceso Gestión de TIC debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la entidad y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.

f) El proceso Gestión de TIC debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de la entidad, ya sea cuando son dados de baja o cambian de usuario.

g) El proceso Gestión de Recursos Físicos debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones del Instituto cuente con la autorización documentada y aprobada previamente por el área.

h) El proceso Gestión de Recursos Físicos debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la entidad y posean las pólizas de seguro correspondientes.

i) El proceso Gestión de TIC es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos del Instituto.

j) Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios y personal provisto por terceras partes deben acoger las instrucciones técnicas que proporcione el proceso Gestión de TIC.

k) Cuando se presente una falla o problema de hardware o software u otro recurso tecnológico propiedad del Instituto, el usuario responsable debe informar al facilitador del proceso Gestión de TIC, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

l) La instalación, reparación o retiro de cualquier componente de hardware o software.

m) Los equipos de cómputo, bajo ninguna circunstancia, no deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.

n) Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.

o) Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

p) En caso de pérdida o robo de un equipo de cómputo, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.
q) Los funcionarios de la entidad y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

POLÍTICA DE USO ADECUADO DE INTERNET

El Instituto, consciente de la importancia del servicio de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad.

Elementos a considerar:

a) El proceso Gestión de TIC debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso que sean establecidos.
b) El proceso Gestión de TIC debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
c) El proceso Gestión de TIC debe monitorear continuamente el canal o canales del servicio de Internet.
d) El proceso Gestión de TIC debe establecer e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
e) El proceso Gestión de TIC debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet.
f) Los usuarios del servicio de Internet de El Instituto deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.
g) Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

h) No está permitido el acceso a páginas relacionadas con ofertas abusivas de publicidad no relacionadas con los fines del Instituto, la pornografía, el consumo de drogas o de alcohol, webproxys, hacking o cualquier otra página web que vaya en contra de la ética, la moral, las leyes vigentes o políticas establecidas en este documento.

i) Sin perjuicio del uso de medios oficiales de comunicación pública de la entidad, los usuarios del servicio de internet institucional no podrán, en horas laborales y con recursos de la entidad, acceder o usar servicios interactivos o mensajería instantánea de carácter personal como Facebook, Kazaa, MSN, Yahoo, Skype, Net2phome y otros similares, que tengan como objetivo crear comunidades para intercambiar información personal, o bien para fines diferentes a las actividades propias del Instituto.

j) En equipos tecnológicos de propiedad, o en uso formal del Instituto, no está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el facilitador del proceso Gestión de TIC o a quien haya sido delegado de forma explícita por la Gerencia del Instituto para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso, en los términos de este instrumento.

POLÍTICA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

En cumplimiento de la de Ley 1581 de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales, El Instituto propende por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establece los términos, condiciones y finalidades para las cuales IMVIYUMBO, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que, en algún momento, por

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

razones de la actividad que desarrolla la entidad, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, El Instituto exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales. Así mismo, busca proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información de la entidad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la entidad y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

Elementos a Considerar:

a) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la entidad.
b) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.
c) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.
d) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.
e) Las Unidades de Gestión que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.
f) Planeación debe establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, proveedores y demás terceros de El Instituto, de los cuales reciba y administre información.
g) El proceso Gestión de TIC debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, proveedores u otras

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

h) Los usuarios y funcionarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la entidad o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.

i) Es deber de los usuarios y funcionarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

j) Los usuarios de los portales de El Instituto deben asumir la responsabilidad individual sobre la clave de acceso a dichos portales que se les suministre; así mismo, deben cambiar de manera periódica esta clave de acceso.

DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

El Instituto con el propósito de garantizar la disponibilidad de la información y mantener los servicios orientados con el objetivo de la entidad y los ofrecidos externamente, a decidió crear una política para proveer el funcionamiento correcto y seguro de la información y medios de comunicación.

POLÍTICA DE CONTINUIDAD, CONTINGENCIA Y RECUPERACIÓN DE LA INFORMACIÓN

El Instituto proporcionará los recursos suficientes para facilitar una respuesta efectiva a los funcionarios y para los procesos en caso de contingencia o eventos catastróficos que se presenten en la entidad y que afecten la continuidad de su operación y servicio.

COPIAS DE SEGURIDAD

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Proceso de Gestión de Tecnologías. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

Las dependencias de El Instituto deben realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas. Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

El proceso Gestión de TIC debe proveer las herramientas para que las dependencias puedan administra la información y registros de copias de seguridad. La (el) profesional especializado con funciones de Control Interno debe efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad. La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios.

Elementos a considerar:

a) Control Interno debe reconocer las situaciones que serán identificadas como emergencia o desastre para la entidad, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.
b) Control Interno debe liderar los temas relacionados con la continuidad de la entidad y la recuperación ante desastres
c) Control Interno debe realizar los análisis de impacto en la entidad y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.
d) Control Interno debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información del Instituto.
e) Control Interno, debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de entidad, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

FASE DE IMPLEMENTACIÓN

Para el desarrollo de esta fase IMVIYUMBO debe utilizar los resultados de la etapa de Planificación y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

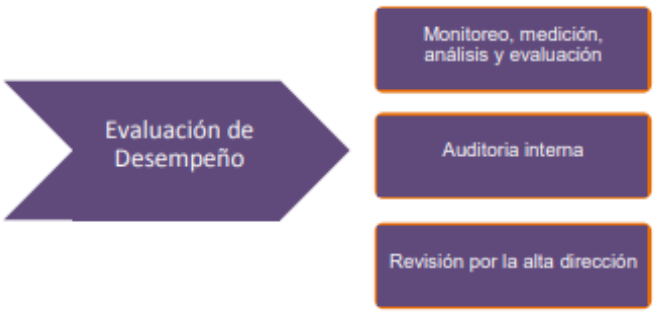
El alcance del MSPI permite a IMVIYUMBO definir los límites sobre los cuales se implementará la seguridad y privacidad en la Institución. Este enfoque es por procesos y debe extenderse a toda la Entidad. En la fase de implementación se realizan las siguientes metas de acuerdo al resultado de la planeación.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

IMPLEMENTACIÓN			
Actividad	**Instrumento**	**Resultado**	**Responsable**
Realizar la Planificación y Control Operacional.	Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Proceso Gestión de Tecnologías.
Implementar el plan de tratamiento de riesgos en la entidad	Documento con la declaración de aplicabilidad. Documento con el plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	Proceso Gestión de Tecnologías.
Generar Indicadores De Gestión.	Guía No 9 - Indicadores de Gestión SI.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	Proceso Gestión de Tecnologías.

FASE DE EVALUACIÓN Y DESEMPEÑO

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.



Fase de Evaluación de desempeño

En aplicación del principio de auto control, el líder del proceso TIC de la Entidad diseñará un programa de seguimiento a las actividades que se incorporan al presente instrumento de gestión, que será comunicado a los involucrados. El seguimiento tendrá como

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

fundamento un plan de acción anual que para cada vigencia fiscal realizará la Alta dirección del Instituto Municipal, debiendo incorporarlo al plan institucional de gestión anual.

Corresponde al jefe de la Oficina de Control Interno realizar las actividades de seguimiento o de auditoría que considere necesarias, para evaluar el cumplimiento del plan de acción anual del presente instrumento de gestión. De cada acto de seguimiento o control, se dejará constancia para conocimiento de la Gerencia.

Si de las labores de seguimiento se evidencia el incumplimiento de una de las actividades del presente Plan; se deberá de suscribir plan de mejora que contenga las acciones correctivas necesarias, para atender los fines propuestos en esta política institucional.

EVALUACIÓN DE DESEMPEÑO			
Actividad	**Instrumento**	**Resultado**	**Responsable**
Hacer el Plan de revisión y seguimiento, a la implementación del MSPI.	Guía No 16 – Evaluación del desempeño.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	Control Interno.
Realizar el Plan de Ejecución de Auditorias,	Guía No 15 – Guía de Auditoría	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.	Control Interno.

FASE DE MEJORA CONTINUA

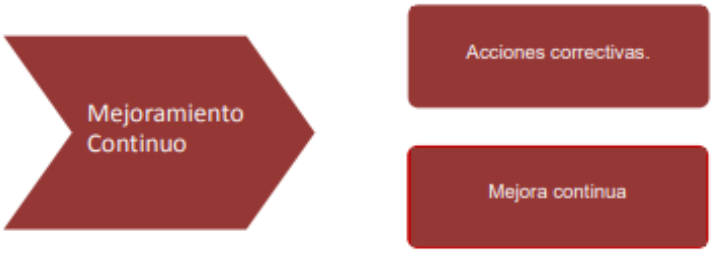
En esta fase la Institución consolidará los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

En esta fase es la entidad definirá y ejecutará el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño.

Este plan incluye:

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

- ✓ Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.
- ✓ Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.



Fase de mejoramiento continúo

MEJORA CONTINUA			
Actividad	**Instrumentos**	**Resultado**	**Responsable**
Crear el Plan de mejora continua.	Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI. Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI. Guía No 17 – Mejora Continua	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.	Proceso Gestión de Tecnologías.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

GUÍAS MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Los siguientes documentos brindados por el MINTIC serán tenidos en cuenta en la implementación el Modelo de Seguridad y Privacidad de la Información en IMVIYUMBO:

- ✓ Modelo de Seguridad y Privacidad de la Información.
- ✓ Instructivo Herramienta de Diagnostico.
- ✓ Herramienta de Diagnostico.
- ✓ Guía Mi pymes.
- ✓ Guía 1 Metodología de pruebas de efectividad.
- ✓ Guía 2 Política General MSPI v1.
- ✓ Guía 3 Procedimientos de Seguridad y Privacidad de la Información.
- ✓ Guía 4 Roles y responsabilidades de seguridad y privacidad de la información.
- ✓ Guía 5 Gestión de Activos.
- ✓ Guía 6 Gestión Documental.
- ✓ Guía 7 Gestión de Riesgos.
- ✓ Guía 8 Controles de Seguridad.
- ✓ Guía 9 Indicadores Gestión SI.
- ✓ Guía 10 Continuidad de TI.
- ✓ Guía 11 Impacto Negocio.
- ✓ Guía 12 Seguridad en la Nube.
- ✓ Guía 13 Guía De Evidencia Digital.
- ✓ Guía 14 Plan de comunicación, sensibilización y capacitación.
- ✓ Guía 15 Auditoria.
- ✓ Guía 16 Evaluación del Desempeño.
- ✓ Guía 17 Mejora Continua.
- ✓ Guía 18 Lineamientos terminales de áreas financieras entidades públicas.
- ✓ Guía 19 Gestión de Incidentes.

PLAN DE COMUNICACIÓN

Mediante socialización a todos los servidores del estado, el Instituto dará a conocer el contenido del presente Plan y las Políticas de Seguridad; así mismo se deberá informar en el momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al plan. Todos los involucrados con el Instituto deben conocer la existencia de las Políticas y la obligatoriedad de su cumplimiento. La ubicación física del documento estará a cargo del Sistema de Gestión Documental para que sean consultados en el momento que se requieran, igualmente estarán alojados en la página de la entidad www.imviyumbo.gov.co.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.

ULTIMA ACTUALIZACIÓN: 2020		
Actualizó: JHON ALEXANDER PINO	Revisó: EVELYN LOAIZA GÓMEZ	Aprobó: EDWIN CORTAZAR VILLABÓN
CARGO: PERSONAL DE APOYO GESTIÓN DE TECNOLOGÍAS (CONTRATISTA)	CARGO: JEFE OFICINA ASESORA DE PLANEACIÓN	CARGO: GERENTE

ANEXO

a). Control de Cambios: *Nota: Los documentos obsoletos se les da de baja del Sistema Integrado de Gestión Institucional.*

Versión	Fecha (dd/mm/aa)	Aprobado por:	Descripción de la actualización
1	29/06/2018	Gilma Mancilla Angulo (Gerente)	Creación del Documento.
2	02/03/2020	Uriel Urbano Urbano (Gerente)	Actualización de logo e imagen corporativa.
3	04/05/2021	Uriel Urbano Urbano (Gerente)	Cambio de código en el Sistema Integrado de Gestión Institucional, a causa de la creación del Proceso Gestión de Tecnologías.
4	23/01/2023	Uriel Urbano Urbano (Gerente)	Actualización vigencia 2023.
5	24/01/2024	Edwin Cortazar Villabón (Gerente)	Actualización vigencia 2024.

Este documento es propiedad del Instituto de Reforma Urbana y Vivienda de Interés Social de Yumbo IMVIYUMBO. Prohibida su reproducción por cualquier medio, sin previa autorización de la Gerencia.