PRESIDENCIA MUNICIPAL DE TIZAYUCA, HIDALGO

LINEAMIENTOS PARA LA ADQUISICIÓN, MANTENIMIENTO, SOPORTE, DESARROLLO, USO Y DESECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Municipio de Tizayuca, Hidalgo.

Unidad de Innovación y Transformación Digital

Contenido

Capítulo I. Introducción

En el contexto de la modernización administrativa y de la gestión eficiente y responsable de los recursos tecnológicos, se presentan los *Lineamientos para la Adquisición, Mantenimiento, Soporte, Desarrollo, Uso y Disposición Final de las Tecnologías de la Información*. Este instrumento normativo tiene como propósito establecer un marco regulador claro, ordenado y transparente para todo el ciclo de vida de los recursos informáticos de la Administración Pública Municipal, asegurando que su gestión se realice de manera eficiente, segura y en estricto cumplimiento de la normatividad vigente.

La correcta aplicación de estos lineamientos permite fortalecer la capacidad institucional para proteger los activos de información, garantizar la continuidad de los servicios públicos esenciales y salvaguardar la integridad, disponibilidad y confidencialidad de los datos institucionales. Con ello, se contribuye de manera directa al cumplimiento de los objetivos estratégicos y a la consolidación de las responsabilidades del Municipio de Tizayuca, Hidalgo, reafirmando su compromiso con la innovación, la transparencia y la resiliencia operativa.

Capítulo II. Objetivo General

Establecer el marco normativo y procedimental que regule de manera ordenada, eficiente y transparente la adquisición, mantenimiento, soporte, desarrollo, uso y disposición final de las Tecnologías de la Información de la Presidencia Municipal de Tizayuca, Hidalgo; garantizando su adecuada administración, seguridad y operatividad, en estricto apego a la normatividad vigente, con el propósito de optimizar el aprovechamiento de los recursos tecnológicos, proteger los activos de información institucional, asegurar la continuidad de los servicios públicos y fortalecer la capacidad operativa y de respuesta de la administración municipal.

Capítulo III. Marco Legal

Los ordenamientos jurídicos y administrativos vigentes que regulan la operación de las actividades y tareas específicas en materia de tecnologías de la información dentro de la administración Pública Municipal, sirven como base normativa para establecer y aplicar los procedimientos, políticas y controles institucionales.

El presente documento se sustenta en lo dispuesto en el **Título Segundo** del *Marco Estatal de Control Interno para el Sector Público del Estado de Hidalgo*, **Capítulo I** “Estructura del Marco”, **Numeral 9** “Normas generales, principios y elementos de control interno”, **Apartado Tercero** “Actividades de control”, **Numeral 11**:

“Seleccionar y desarrollar actividades de control basadas en las Tecnologías de la Información y Comunicaciones (TIC)”.

Asimismo, se observa lo señalado en los **Lineamientos de Control Interno del Municipio de Tizayuca Hidalgo**, en el apartado *“Diseño de la adquisición, desarrollo y Mantenimiento de las TIC´s”*, así como de “revisiones periódicas a las actividades de Control” numeral 3.04, y al artículo 31 sección V, VI, y VII.

Capítulo IV. Adquisición de tecnologías de la información.

I. Evaluación de las necesidades de cada Dependencia y Unidad Administrativa.

Previo a la adquisición de equipos, se realiza un análisis detallado de las necesidades específicas de cada puesto de trabajo por medio de un levantamiento físico de los bienes informáticos, considerando las funciones asignadas y los requerimientos operativos. Dicho análisis contempla aspectos como el tipo y complejidad de las tareas a desempeñar, el software y licencias necesarias, la capacidad de almacenamiento requerida, así como la durabilidad y vida útil esperada del equipo, con el fin de garantizar que los recursos adquiridos sean idóneos, eficientes y acordes a las demandas institucionales.

II. Presupuesto.

Se establece un presupuesto para la adquisición de equipos, el cual deberá ser ejercido por la Unidad o Dependencia concentradora con base en las necesidades previamente justificadas por cada dependencia y Unidad Administrativa solicitante. La autorización de dicho gasto estará condicionada al visto bueno y dictamen técnico emitido por la Instancia Municipal competente de realizar Innovación, Soporte y Mantenimiento a los bienes informáticos, a fin de garantizar que la adquisición sea pertinente, eficiente y alineada con los estándares tecnológicos y normativos de la Presidencia Municipal de Tizayuca, Hidalgo.

III. Investigación de opciones.

La Instancia Municipal competente de realizar Innovación, Soporte y Mantenimiento a los bienes informáticos como área técnica y solicitante, realiza una investigación comparativa de diferentes marcas, modelos y especificaciones técnicas del Hardware y software de los equipos de cómputo, con el fin de garantizar que los equipos de cómputo seleccionados cumplan plenamente con los requerimientos operativos de cada usuario, en función de las responsabilidades y funciones asignadas a su puesto.

IV. Actualización futura.

Se contempla la viabilidad de futuras actualizaciones como criterio de selección. Por ello, se prioriza la adquisición de equipos que permitan la expansión de memoria, la sustitución o mejora de componentes, así como la disponibilidad de puertos y conexiones adecuadas, a fin de prolongar su vida útil, optimizar su rendimiento y garantizar su adaptación a las necesidades tecnológicas emergentes de la institución.

V. Soporte técnico.

Verifica la disponibilidad de soporte técnico y garantías ofrecidas por el fabricante o el vendedor. Un buen soporte técnico puede ser crucial en caso de problemas o necesidad de asistencia.

VI. Seguridad.

Cuando los analistas de soporte de la Unidad de Innovación y Transformación Digital realizan la configuración de los equipos de cómputo de nueva adquisición, se verifica que cuenten con las medidas de seguridad necesarias, incluyendo sistemas de protección contra virus, malware y otras amenazas cibernéticas, así como mecanismos de cifrado de datos que salvaguarden la integridad, confidencialidad y disponibilidad de la información institucional.

VII. Capacitación.

Si es necesario, se planifica la capacitación para los usuarios en el uso adecuado de los nuevos equipos de cómputo adquiridos con el fin de hacer un buen uso.

Capítulo V. Mantenimiento, soporte, desarrollo y uso de las tecnologías de la información.

Los siguientes lineamientos tienen como finalidad establecer procedimientos claros y seguros para el desecho, disposición final o donación de los bienes tecnológicos en desuso de la presidencia municipal, garantizando la protección de la información pública y personal contenida en los equipos, así como el cumplimiento de la normatividad aplicable en materia de transparencia, medio ambiente y administración de recursos públicos.

VIII. Clasificación de la información.

a) Los titulares de cada dependencia y unidad administrativa deben informar a sus colaboradores de la clasificación de la información a su cargo para su adecuado tratamiento.

Nivel de Clasificación	Descripción	Ejemplos de Información	Medidas de Protección Recomendadas
Confidencial	Información cuyo acceso no autorizado podría generar daños graves a la operación, a la seguridad de los sistemas o a la reputación institucional.	Bases de datos de ciudadanos, credenciales de acceso a sistemas, claves criptográficas, expedientes legales en curso, información financiera no pública.	Cifrado de datos, acceso restringido con autenticación multifactor, almacenamiento en servidores seguros, respaldo en medios cifrados, políticas estrictas de acceso y auditoría.
Restringida	Información cuyo acceso no autorizado podría generar afectaciones moderadas a los procesos institucionales o a la prestación de servicios.	Correspondencia interna, reportes de operación, manuales técnicos, listas de personal, actas administrativas.	Control de acceso por usuario, contraseñas robustas, protección contra malware, respaldo periódico en entornos controlados.
Pública	Información que puede ser divulgada sin riesgo significativo para la institución.	Comunicados oficiales, información de transparencia, directorios públicos, normatividad publicada en portales.	Disponibilidad en portales institucionales, control de versiones, verificación de integridad antes de publicación.

b) Todo usuario es responsable del resguardo de datos, debe confirmar que la información esté protegida para asegurar su integridad y confidencialidad, acorde a su clasificación.
c) Todo trabajador que tenga acceso a información clasificada como *confidencial* o *restringida* deberá utilizarla exclusivamente para fines relacionados con el ejercicio de sus funciones y responsabilidades institucionales. En especial, deberá garantizar la protección y resguardo de los datos personales, absteniéndose de divulgarlos, transferirlos o ponerlos a disposición de terceros sin el consentimiento expreso, previo e informado de la persona titular de los mismos.
d) Todos los trabajadores (usuarios) que hacen uso de información clasificada como restringida o confidencial, evitarán que sea accedida por personas no autorizadas.

IX. Buen uso de los activos informáticos.

a) Los usuarios (trabajadores) a quienes se les haya asignado un activo informático de manera personal para el desarrollo de sus funciones serán los únicos responsables de su correcto uso, conservación y del manejo de la información que en él se resguarde. En este sentido, deberán abstenerse de compartir el equipo con terceros. En caso de ser necesario compartirlo o prestarlo, dicho uso deberá realizarse exclusivamente para fines laborales, permaneciendo en todo momento la responsabilidad sobre el activo y su contenido en la persona a la que fue asignado.
b) Toda movilización de activo informático dentro o fuera de las instalaciones de la institución es responsabilidad del usuario resguardante, y deberá informar de este cambio a la Secretaría General Municipal, a la instancia Municipal encargada del Patrimonio Municipal, así como a la Instancia Municipal competente de realizar Innovación, Soporte y Mantenimiento a los bienes informáticos.

X. Prestación de servicios por terceros.

a) Todo proveedor que proporcione servicios informáticos de la Presidencia Municipal de Tizayuca, Hidalgo, y que tenga acceso a información reservada y/o confidencial, deberá apegarse a las disposiciones de las leyes, reglamentos y demás instrumentos normativos relacionados con acceso a la información pública y protección de datos personales y contar con acuerdos de no divulgación ni uso que perjudique a la misma.
b) Todo servicio informático otorgado por terceros debe ser monitoreado y revisado por la persona responsable de su contratación, para asegurar que se cumplan con los términos estipulados en los acuerdos, leyes, reglamentos y demás instrumentos normativos establecido.

XI. Protección contra código malicioso (virus y malware).

a) Todo bien informático institucional debe contar con software antivirus y antimalware definido por la Instancia Municipal competente de realizar Innovación, Soporte y Mantenimiento a los bienes informáticos (Kaspersky o Microsoft Defender), así como estar protegido por el Firewall (Fortinet). Si el software antivirus no cubre a la plataforma utilizada, el personal notificará a la Unidad encargada para buscar una alternativa de solución.
b) Todo usuario que identifique una anomalía en su equipo de cómputo o falla en la red, deberá reportarla de inmediato a la instancia municipal competente de realizar soporte y mantenimiento a los bienes informáticos usando la plataforma de Soporte Técnico en el Url https://devs.tizayuca.gob.mx/soporte-tecnico-sistemas/?wpsc-

section=ticket-list, por medio de un ticket de soporte técnico, con el fin de dar pronta solución a la problemática.

XII. Servicios informáticos en la red.

a) Todo el personal, estudiantes que realizan prestación de servicio y terceros que hacen uso de los bienes informáticos son responsables del buen uso de los servicios informáticos alojados en nuestras instalaciones y en la nube, asignados para realizar sus funciones administrativas.
b) Sólo el Personal de la Instancia Municipal competente de realizar Innovación, Soporte y Mantenimiento a los bienes informáticos queda facultado para acceder a los equipos de cómputo institucionales, para:
    a. Ejecutar las tareas del procedimiento de mantenimiento preventivo y correctivo.
    b. Realizar modificaciones a los sistemas operativos.
    c. Realizar una revisión de seguridad informática, dictamen técnico y descartar uso indebido (daños intencionales a información del software) del equipo de cómputo.
c) Corresponde a cada titular de las dependencias y unidades administrativas la responsabilidad de autorizar el acceso a los equipos de cómputo que les hayan sido asignados, así como de aprobar cualquier modificación irreversible en los sistemas, tales como el formateo, la eliminación de información o cualquier otra acción que pueda comprometer la integridad de los datos.
d) Ninguna persona debe alterar o destruir la información que reside en los equipos de cómputo y servidores sin el consentimiento explícito del titular de la Dependencia o Unidad Administrativa.
e) Todas las cuentas de usuario y su respectiva contraseña de acceso a los sistemas, equipos de cómputo y servicios de información de la Administración Pública Municipal de Tizayuca, Hidalgo son personales, permitiéndose el uso bajo su responsabilidad, única y exclusivamente durante la vigencia de los derechos del usuario.
f) El equipo de cómputo institucional (computadoras de escritorio, computadoras portátiles, escáner, impresoras, etc.), serán configurados solamente por personal de la Instancia Municipal competente de realizar Innovación, Soporte y Mantenimiento a los bienes para brindar acceso a la red. Todo usuario se abstendrá de realizar cambios en configuraciones de esta naturaleza, en caso de falla o error de acceso a internet por esta causa, será el único responsable.
g) A toda persona que deje de laborar o tener relación con el ayuntamiento, le será cancelado su acceso de manera definitiva a los recursos informáticos institucionales, por lo cual se deberá comunicar a la Instancia Municipal competente de realizar Innovación, Soporte y Mantenimiento a los bienes

informáticos para informar toda alta, baja o cambio del personal para que se tomen las medidas correspondientes de privilegios de acceso a los servicios de red.

XIII. Uso de Internet.

a) El servicio de Internet a través de las redes institucionales se considera como herramienta de trabajo, por lo que todo usuario deberá utilizarlo exclusivamente para apoyo a las actividades administrativas que desempeñan.
b) Todo titular de la Dependencia o Unidad Administrativa puede solicitar la restricción total o parcial de acceso a Internet del personal a su cargo, considerando para ello las funciones laborales que éstos realizan.
c) Todo usuario que descargue información y archivos de Internet mediante el navegador web u otro medio, debe de omitir descargar archivos de dudosa procedencia. Los archivos descargados de Internet pueden contener virus o software malicioso que pongan en riesgo la información del equipo de cómputo de la persona, e incluso de la Institución.

Capítulo VI. Desecho de las tecnologías.

XIV. Verificación de bienes en desuso o inservibles

La Instancia Municipal competente de realizar Innovación, Soporte y Mantenimiento a los bienes informáticos llevará a cabo una evaluación técnica integral de los bienes informáticos que presenten fallas o desperfectos. Con base en dicha revisión, se emitirá un dictamen técnico en el que se detallarán las condiciones y daños identificados, así como la viabilidad de su reparación. En caso de que el bien sea declarado irreparable o antieconómico para su restauración, será clasificado como desecho tecnológico, procediéndose a su disposición conforme a la normativa vigente.

XV. Recolección.

La instancia Municipal encargada del Patrimonio Municipal establece puntos de recolección dedicados para los equipos tecnológicos en desuso o inservibles en lugares estratégicos, como centros de reciclaje, tiendas de electrónica o centros comunitarios.

XVI. Separación.

La Instancia Municipal competente de realizar Innovación, Soporte y Mantenimiento a los bienes informáticos será la encargada de verificar y recuperar las refacciones que resulten funcionales de aquellos bienes informáticos que hayan concluido su vida útil. Asimismo, deberá garantizar que, desde el momento en que se proceda a su disposición final, los

desechos tecnológicos sean segregados de otros tipos de residuos, a fin de cumplir con las disposiciones ambientales aplicables y fomentar el aprovechamiento responsable de componentes reutilizables.

XVII. Almacenamiento temporal.

Proporciona contenedores adecuados y seguros para el almacenamiento temporal de desechos tecnológicos antes de su recogida.

XVIII. Clasificación.

Clasifica los desechos tecnológicos según su tipo, como dispositivos electrónicos, baterías, cables, placas de circuitos, etc.

Tabla de clasificación de desechos tecnológicos

Categoría	Ejemplos de Componentes	Riesgos Asociados	Manejo Recomendado
Dispositivos electrónicos completos	Computadoras, laptops, impresoras, escáneres, teléfonos IP, proyectores	Contienen metales pesados, plásticos no biodegradables y componentes electrónicos	Recolección separada y envío a centros de reciclaje especializados
Baterías y acumuladores	Baterías de litio, níquel-cadmio, plomo-ácido, UPS	Altamente contaminantes, riesgo de fugas y explosiones	Almacenamiento en contenedores aislados y disposición mediante gestor autorizado
Cables y conectores	Cables de alimentación, de datos, HDMI, USB, conectores RJ45, adaptadores	Contienen cobre y recubrimientos plásticos	Separación por tipo y reciclaje para recuperación de metales
Placas y tarjetas electrónicas	Tarjetas madre, tarjetas gráficas, tarjetas de red, placas de circuito impreso	Contienen metales pesados, soldaduras con plomo y componentes electrónicos delicados	Desmontaje seguro y envío a recicladores certificados
Componentes de almacenamiento	Discos duros, SSD, memorias RAM, unidades ópticas	Pueden contener información confidencial, riesgo de filtración de datos	Borrado seguro de datos y destrucción física antes del reciclaje
Periféricos	Teclados, ratones, cámaras web, bocinas	Bajo nivel de riesgo químico, pero alto en volumen de desecho	Recolección separada y reciclaje de plásticos y metales
Monitores y pantallas	Monitores LCD, LED, plasma	Contienen mercurio y otros elementos tóxicos	Manejo especial y disposición mediante gestor autorizado

Tabla de clasificación de desechos tecnológicos			
Categoría	Ejemplos de Componentes	Riesgos Asociados	Manejo Recomendado
Fuentes de alimentación	Cargadores, fuentes ATX, adaptadores de corriente	Riesgo eléctrico y de incendio	Desensamble y reciclaje por partes
Consumibles electrónicos	Cartuchos de tinta, tóner, cintas	Contaminantes químicos	Recolección en puntos de acopio autorizados y reciclaje especializado

XIX. Desmantelamiento seguro para reciclaje o reutilización.

Los analistas de soporte de la Instancia Municipal competente de realizar Innovación, Soporte y Mantenimiento a los bienes informáticos están capacitados para desmontar equipos tecnológicos de manera segura, evitando la liberación de sustancias peligrosas.

XX. Informes y seguimiento.

La Instancia Municipal encargada del Patrimonio Municipal y la Instancia Municipal competente de realizar Innovación, Soporte y Mantenimiento a los bienes informáticos llevan un registro detallado de la cantidad y tipo de desechos tecnológicos manejados, así como de los métodos utilizados para su tratamiento.

XXI. Investigación y desarrollo.

Invierte en investigaciones para desarrollar métodos más eficientes y seguros de manejo de desechos tecnológicos.

Elaboró	Revisó	Aprobó
P.L. Ariadna Natali Meneses Juárez Asistente Administrativo de la Unidad de Innovación y Transformación Digital	Tec. Javier Alazañes Sánchez Titular de la Unidad de Innovación y Transformación Digital	Ing. Gretchen Aline Atilano Moreno Presidenta Municipal Constitucional del Tizayuca, Hidalgo

Glosario de Términos

Activo informático: Bien material o inmaterial relacionado con el uso de las tecnologías de la información que posee valor para la organización. Incluye equipos de cómputo, servidores, redes, software, licencias, bases de datos y cualquier recurso tecnológico asignado para el cumplimiento de funciones institucionales.

Analistas de soporte: Profesionales responsables de brindar asistencia técnica y operativa a los usuarios en el uso de equipos de cómputo, sistemas informáticos, redes y aplicaciones.

Área solicitante: Se entiende por este término el conjunto de dependencias y unidades administrativas que conforman la estructura orgánica de la Presidencia Municipal de Tizayuca, Hidalgo.

Área técnica: Es la unidad responsable de planificar, ejecutar y supervisar las acciones de mantenimiento preventivo y correctivo, así como de proporcionar soporte técnico especializado a los equipos de cómputo, dispositivos periféricos y demás bienes informáticos propiedad de la institución.

Desecho tecnológico: Todo equipo, componente o dispositivo electrónico que ha cumplido su vida útil o ha quedado obsoleto, incluyendo computadoras, periféricos, baterías, cables y placas de circuitos.

Firewall: Sistema de seguridad de red que filtra y controla el tráfico entrante y saliente entre redes internas y externas, de acuerdo con un conjunto de reglas predefinidas. Su propósito es prevenir accesos no autorizados y proteger la integridad de los sistemas informáticos.

Kaspersky: Solución de seguridad informática desarrollada por la empresa Kaspersky Lab, especializada en la protección contra virus, malware, ransomware y amenazas cibernéticas, mediante funciones como análisis en tiempo real, control de aplicaciones y filtrado web.

Malware: Software malicioso diseñado para infiltrarse, dañar o interrumpir el funcionamiento de un sistema informático sin el consentimiento del usuario. Incluye virus, troyanos, ransomware, spyware y otros programas nocivos que comprometen la seguridad y privacidad de la información.

Microsoft Defender: Plataforma de seguridad desarrollada por Microsoft para proteger sistemas operativos Windows contra malware, amenazas en la nube, ataques de phishing y otras vulnerabilidades, integrando herramientas de análisis, control y respuesta.

Multifactor: Método de autenticación que requiere dos o más elementos de verificación independientes para conceder acceso a un sistema o servicio. Combina factores como contraseñas, códigos enviados a dispositivos móviles, huellas digitales o reconocimiento facial, con el fin de reforzar la seguridad.

Software: Conjunto de programas, aplicaciones, sistemas operativos y utilidades que permiten la operación y el control de los dispositivos electrónicos. Puede clasificarse en software de sistema, de aplicación o de desarrollo, y es indispensable para la ejecución de tareas, el manejo de datos y el funcionamiento de la infraestructura tecnológica institucional.

Usuario: Personas autorizadas para acceder y utilizar los recursos informáticos y tecnológicos de la institución, en función de sus responsabilidades laborales.

Área técnica: Es la unidad responsable de planificar, ejecutar y supervisar las acciones de mantenimiento preventivo y correctivo, así como de proporcionar soporte técnico especializado a los equipos de cómputo, dispositivos periféricos y demás bienes informáticos propiedad de la institución.

Analistas de soporte: Profesionales responsables de brindar asistencia técnica y operativa a los usuarios en el uso de equipos de cómputo, sistemas informáticos, redes y aplicaciones.

Área solicitante: Se entiende por este término el conjunto de dependencias y unidades administrativas que conforman la estructura orgánica de la Presidencia Municipal de Tizayuca, Hidalgo.

Malware: Software malicioso diseñado para infiltrarse, dañar o interrumpir el funcionamiento de un sistema informático sin el consentimiento del usuario. Incluye virus, troyanos, ransomware, spyware y otros programas nocivos que comprometen la seguridad y privacidad de la información.

Software: Conjunto de programas, aplicaciones, sistemas operativos y utilidades que permiten la operación y el control de los dispositivos electrónicos. Puede clasificarse en software de sistema, de aplicación o de desarrollo, y es indispensable para la ejecución de tareas, el manejo de datos y el funcionamiento de la infraestructura tecnológica institucional.

Activo informático: Bien material o inmaterial relacionado con el uso de las tecnologías de la información que posee valor para la organización. Incluye equipos de cómputo, servidores, redes, software, licencias, bases de datos y cualquier recurso tecnológico asignado para el cumplimiento de funciones institucionales.

Multifactor: Método de autenticación que requiere dos o más elementos de verificación independientes para conceder acceso a un sistema o servicio. Combina

factores como contraseñas, códigos enviados a dispositivos móviles, huellas digitales o reconocimiento facial, con el fin de reforzar la seguridad.

Usuarios: Personas autorizadas para acceder y utilizar los recursos informáticos y tecnológicos de la institución, en función de sus responsabilidades laborales.

Kaspersky: Solución de seguridad informática desarrollada por la empresa Kaspersky Lab, especializada en la protección contra virus, malware, ransomware y amenazas cibernéticas, mediante funciones como análisis en tiempo real, control de aplicaciones y filtrado web.

Microsoft Defender: Plataforma de seguridad desarrollada por Microsoft para proteger sistemas operativos Windows contra malware, amenazas en la nube, ataques de phishing y otras vulnerabilidades, integrando herramientas de análisis, control y respuesta.

Firewall: Sistema de seguridad de red que filtra y controla el tráfico entrante y saliente entre redes internas y externas, de acuerdo con un conjunto de reglas predefinidas. Su propósito es prevenir accesos no autorizados y proteger la integridad de los sistemas informáticos.

Desecho tecnológico: Todo equipo, componente o dispositivo electrónico que ha cumplido su vida útil o ha quedado obsoleto, incluyendo computadoras, periféricos, baterías, cables y placas de circuitos.

Usuario: Persona, entidad o sistema que accede, interactúa o utiliza recursos, servicios o aplicaciones informáticas, ya sea de manera directa o a través de interfaces, con el fin de ejecutar tareas, consultar información o administrar sistemas.