Tizayuca
Ciudad Próspera
2024 - 2027

BICENTENARIO TIZAYUCA 1826 2026

IMDUYV
INSTITUTO MUNICIPAL DE DESARROLLO URBANO Y VIVIENDA

LINEAMIENTOS DE USO, ADMINISTRACIÓN Y SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN DEL INSTITUTO MUNICIPAL DE DESARROLLO URBANO Y VIVIENDA.

Con fundamento en el artículo 115 fracción II de la Constitución Política de los Estados Unidos Mexicanos, 141 fracción II de la Constitución Política del Estado de Hidalgo, 7, 56 fracción I inciso b), 60 fracción I inciso a), 112 y 113 de la Ley Orgánica Municipal para el Estado de Hidalgo y 1, 6, 11 fracción IV y VII del Decreto por el que se crea el Organismo Público Descentralizado denominado Instituto Municipal de Desarrollo Urbano y Vivienda y 27 fracción IV y VII del Reglamento Interior del Instituto Municipal de Desarrollo Urbano y Vivienda ha tenido a bien de expedir el siguiente documento.

ING. GRETCHEN ALYNE ATILANO MORENO, PRESIDENTA MUNICIPAL CONSTITUCIONAL DEL MUNICIPIO DE TIZAYUCA, HIDALGO Y PRESIDENTA DE LA JUNTA DE GOBIERNO DEL INSTITUTO MUNICIPAL DE DESARROLLO URBANO Y VIVIENDA DEL MUNICIPIO DE TIZAYUCA, EN USO DE LAS FACULTADES QUE LE CONFIEREN LOS ARTÍCULOS 115 FRACCIÓN II DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, 141 FRACCIÓN II DE LA CONSTITUCIÓN POLÍTICA DEL ESTADO DE HIDALGO; Y 7, 56 FRACCIÓN I INCISO B) Y 60 FRACCIÓN I, INCISO A DE LA LEY ORGÁNICA MUNICIPAL PARA EL ESTADO DE HIDALGO; Y CON FUNDAMENTO EN LOS ARTÍCULOS , 115, 122, 123 Y 141 FRACCIÓN II DE LA CONSTITUCIÓN POLÍTICA DEL ESTADO DE HIDALGO, 1, 2, 3, 7 Y 56 FRACCIÓN I, INCISO A), 69, FRACCIÓN IX, 70, 71 FRACCIÓN I INCISO D), 72, 189, 190 Y 191 DE LA LEY ORGÁNICA MUNICIPAL DEL ESTADO; COMO ORGANISMO DESCENTRALIZADO DEL AYUNTAMIENTO DE TIZAYUCA, HIDALGO, Y DEMÁS RELATIVOS APLICABLES, SOMETO A CONSIDERACIÓN DE LA Y LOS INTEGRANTES DE LA JUNTA DE GOBIERNO DE ESTE INSTITUTO, **LINEAMIENTOS DE USO, ADMINISTRACIÓN Y SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN** DEL INSTITUTO MUNICIPAL DE DESARROLLO URBANO Y VIVIENDA, CON BASE EN LOS SIGUIENTES:

CONSIDERANDOS

PRIMERO. Que, derivado de la Vigésima Sexta Sesión Ordinaria del Honorable Ayuntamiento de Tizayuca, Hidalgo, celebrada el 8 de octubre de 2025, se aprobó el Decreto por el que se crea el Organismo Público Descentralizado denominado Instituto Municipal de Desarrollo Urbano y Vivienda, mismo que fue publicado en el Periódico Oficial del Estado de Hidalgo el 2 de diciembre del 2025. Dicho Decreto constituye el acto jurídico mediante el cual se otorga personalidad jurídica y patrimonio propio al Instituto, estableciendo su naturaleza, objetivos y bases de funcionamiento, con lo que se brinda la certeza normativa necesaria para el ejercicio de sus atribuciones y la implementación de sus disposiciones internas.

SEGUNDO. Que el Decreto de creación del IMDUyV establece la obligación de generar, actualizar y armonizar la normativa interna necesaria para garantizar el adecuado funcionamiento institucional, así como para asegurar que la administración, operación y prestación de los servicios se realicen bajo principios de eficiencia, legalidad, transparencia, profesionalismo y responsabilidad.

TERCERO. Que la incorporación, uso y administración de las Tecnologías de la Información y la Comunicación (TIC), así como la seguridad informática, constituyen elementos esenciales para el ejercicio de las atribuciones del Instituto, debido a que permiten la gestión, almacenamiento,

resguardo y protección de información pública y datos personales, por lo que su regulación debe atender los estándares normativos vigentes en la materia.

CUARTO. Que la Ley General de Transparencia y Acceso a la Información Pública; la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados; la Ley General de Responsabilidades Administrativas; la Ley Orgánica Municipal del Estado de Hidalgo; y demás normatividad aplicable, establecen la obligación de los sujetos obligados de proteger la información bajo su resguardo, garantizar medidas de seguridad adecuadas, prevenir vulneraciones, y asegurar el tratamiento correcto de los datos en posesión de las instituciones públicas.

QUINTO. Que el manejo adecuado de los sistemas informáticos, equipos, software, redes, bases de datos, videograbaciones, así como la continuidad operativa en caso de fallas o desastres, constituye un elemento estratégico para la continuidad de las operaciones del Instituto, por lo que deben definirse lineamientos que regulen la administración, uso, resguardo y protección de los activos informáticos, así como las responsabilidades de los servidores públicos en esta materia.

SEXTO. Que es obligación del Instituto implementar medidas técnicas, administrativas y de control que garanticen la integridad, disponibilidad, confidencialidad y trazabilidad de la información a su cargo, así como establecer mecanismos que permitan prevenir incidentes de seguridad, mitigar riesgos, corregir vulnerabilidades y asegurar el cumplimiento de las mejores prácticas y estándares institucionales en materia de tecnologías de la información.

CAPÍTULO I
DISPOSICIONES PRELIMINARES

ARTÍCULO 1. Los Lineamientos de uso, administración y seguridad de las tecnologías de la información y la comunicación son diseñados y documentados para ser implementados en la adquisición, mantenimiento, soporte, desarrollo, uso y desecho de las tecnologías de la información y la comunicación del Instituto Municipal de Desarrollo Urbano y Vivienda (IMDUyV). Por lo cual su principal objetivo es garantizar, promover y preservar los recursos las TIC´S a través de medidas y formas eficientes que deben cumplir cabalmente la persona encargada de Innovación y los Servidores Públicos adscritos al instituto; así se garantizará salvaguardar los sistemas informáticos en caso de desastre.

ARTÍCULO 2. Los presentes lineamientos tienen la finalidad de salvaguardar los equipos de cómputo, videograbaciones, sistemas informáticos, redes, hardware, software y sistemas

operativos usados en el Instituto Municipal de Desarrollo Urbano y Vivienda (IMDUyV) para así garantizar su mantenimiento, funcionamiento y protección a la información de cada uno de ellos. Este documento será de aplicación para la ciudadanía en general y todos los Servidores Públicos del Instituto Municipal de Desarrollo Urbano y Vivienda que desempeñen labores o proporcionen algún tipo de atención o servicio.

Artículo 3. Para efecto de los presentes lineamientos, se entenderá por:

Acceso autorizado: Facultad otorgada por la persona encargada de Innovación o por el titular del área correspondiente para permitir a un usuario ingresar a sistemas, aplicaciones, equipos o información institucional bajo criterios de necesidad operativa.

Activo informático: Recursos de sistemas informáticos, físicos o digitales, necesarios para el desempeño de las funciones de los usuarios, incluyendo computadoras, dispositivos móviles, periféricos y cualquier equipo relacionado con las TIC.

Administrador de sistemas: Persona designada por la persona encargada de Innovación para gestionar la infraestructura tecnológica, garantizar la operatividad de los servicios informáticos y aplicar configuraciones de seguridad.

Almacenamiento institucional: Espacios digitales, físicos o virtuales destinados exclusivamente a guardar información generada en el desempeño de funciones oficiales, incluyendo servidores, repositorios, nubes autorizadas y respaldos.

Autenticación: Proceso mediante el cual un usuario confirma su identidad para acceder a recursos tecnológicos institucionales mediante contraseñas, tokens o mecanismos biométricos autorizados.

Base de datos: Conjunto estructurado de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su uso posterior.

Bitácora de servicio: Registro documental o electrónico en el que se consignan las intervenciones técnicas realizadas a los equipos o sistemas del Instituto, incluyendo fechas, acciones y responsables.

Comodato: Contrato mediante el cual se da o recibe prestado un bien informático que puede usarse sin destruirse, con la obligación de restituirlo.

Configuración institucional: Conjunto de parámetros técnicos definidos por la persona encargada de Innovación para estandarizar la operación segura de equipos, software y redes.

Continuidad operativa: Capacidad del Instituto para mantener o restablecer funciones críticas en caso de fallas, incidentes o desastres que afecten los recursos tecnológicos.

Control de cambios: Procedimiento mediante el cual se autoriza y registra cualquier modificación realizada a hardware, software o infraestructura tecnológica institucional.

Cuenta institucional: Identidad digital asignada a usuarios autorizados para acceder a servicios, aplicaciones o plataformas del Instituto.

Equipo institucional: Todo dispositivo tecnológico que sea propiedad del Instituto, incluyendo computadoras, impresoras, periféricos y dispositivos de red.

Equipo móvil: Activo informático portátil asignado para el desempeño de funciones, como laptops, tabletas o teléfonos inteligentes.

Persona encargada de Innovación: Responsable de la administración, operación, gestión, soporte y seguridad de los recursos tecnológicos del Instituto, así como del cumplimiento de estos Lineamientos.

Evento de seguridad informática: Cualquier incidente, vulneración, anomalía o riesgo que pueda comprometer la integridad, disponibilidad o confidencialidad de sistemas o información institucional.

IMDUyV: Instituto Municipal de Desarrollo Urbano y Vivienda.

Infraestructura tecnológica: Conjunto de redes, servidores, cableado, sistemas eléctricos, hardware y dispositivos que permiten la operación informática del Instituto.

Integridad de la información: Condición que garantiza que los datos institucionales no han sido alterados o manipulados sin autorización.

Mantenimiento preventivo: Acciones programadas por la persona encargada de Innovación para evitar fallas en equipos, sistemas o infraestructura tecnológica.

Mantenimiento correctivo: Acciones destinadas a restaurar el funcionamiento de equipos o sistemas que presentan fallas o daños.

Medio de almacenamiento removible: Dispositivo externo utilizado para almacenar o transferir información, como USB, discos externos, tarjetas SD, CD o DVD.

OIC: Órgano Interno de Control del Instituto.

PRD: Plan de Recuperación de Desastres

Plataforma digital institucional: Conjunto de sistemas, aplicaciones, portales y servicios digitales autorizados para funciones administrativas, técnicas o de atención ciudadana.

Proveedor tecnológico: Persona física o moral que presta servicios de desarrollo, soporte, instalación, mantenimiento o suministro de tecnologías al Instituto, sujeto a estos Lineamientos.

Recuperación de desastres: Procedimiento destinado a restablecer operaciones tecnológicas después de un evento crítico que afecte la infraestructura o la información.

Recurso tecnológico: Cualquier elemento material, digital o lógico que forme parte de los sistemas y servicios tecnológicos institucionales.

Registro de usuarios: Base documental o electrónica administrada por la persona encargada de Innovación que contiene la relación de cuentas, permisos y privilegios activos del personal.

Restricción de acceso: Medida mediante la cual se limita total o parcialmente el uso de servicios o sistemas tecnológicos por motivos de seguridad o disciplina administrativa.

Servicio informático: Bien intangible que satisface necesidades relacionadas con el uso de activos informáticos institucionales.

Sistema informático institucional: Conjunto de aplicaciones, programas o plataformas cuyo uso está autorizado para funciones oficiales.

Software institucional: Programas informáticos con licencia de uso o propiedad del Instituto, autorizados para el desempeño de funciones oficiales.

Software libre: Programas de libre uso o gratuitos, cuya instalación solo puede realizarse previa autorización de la persona encargada de Innovación.

Soporte técnico: Actividades realizadas por personal competente para diagnosticar, corregir y dar seguimiento a fallas en equipos o sistemas.

TIC's: Tecnologías de la Información y las Comunicaciones.

Usuario: Todo servidor público o persona autorizada que haga uso de activos, sistemas o servicios tecnológicos del Instituto para el desempeño de sus funciones.

Videograbación institucional: Registro audiovisual generado por cámaras de seguridad del Instituto

Virus: Programa informático creado para causar daño o alterar equipos, sistemas, redes o información institucional.

CAPÍTULO II.
DE LA INFORMACIÓN, SU RESPALDO Y PROTECCIÓN.

Artículo 4. Es responsable de salvaguardar la información contenida en los equipos de cómputo de este instituto, la persona encargada de Innovación y es quien efectuara respaldos de forma mensual; en base a un plan de trabajo y cronograma establecido.

Artículo 5. Los servidores públicos adscritos al IMDUyV deberán realizar respaldos periódicos de la información generada en el ejercicio de sus funciones, conforme a la organización de carpetas institucionales y a las instrucciones operativas emitidas por la persona encargada de Innovación. El respaldo deberá efectuarse diariamente o con la periodicidad que la naturaleza del área lo requiera, garantizando la preservación y disponibilidad de los datos institucionales.

Artículo 6. Todo servidor público del IMDUyV es responsable del resguardo adecuado de los datos bajo su posesión, debiendo verificar que la información se encuentre protegida conforme a su clasificación, a fin de asegurar su integridad, disponibilidad y confidencialidad. La información podrá conservarse en medios electrónicos, impresos, magnéticos o cualquier otro mecanismo autorizado, siempre que cuente con las medidas de seguridad correspondientes.

Artículo 7. Los servidores públicos del IMDUyV deberán utilizar la información a la que tengan acceso exclusivamente para fines relacionados con el desempeño de sus funciones. Queda estrictamente prohibido comunicar, divulgar o compartir datos personales o información clasificada sin la autorización expresa del superior jerárquico competente. Todo manejo indebido será sujeto a las responsabilidades y sanciones que correspondan.

Artículo 8. El servidor público que acceda a información clasificada como restringida o confidencial será responsable de prevenir su divulgación, uso indebido o acceso por personas no autorizadas.
El tratamiento y custodia de dicha información deberá realizarse conforme a la Ley General de Responsabilidades Administrativas, la normativa aplicable en materia de protección de datos personales y los presentes Lineamientos.

Artículo 9. Para salvaguardar la información contenida en los equipos de cómputo del IMDUyV, todos los datos, archivos y documentos deberán mantenerse cifrados o protegidos mediante contraseñas seguras.
Dichas contraseñas únicamente podrán ser conocidas por la persona encargada de Innovación y por los servidores públicos autorizados de las unidades administrativas correspondientes, conforme a sus funciones y niveles de acceso.

Artículo 10. Los servidores públicos que utilicen equipos personales para realizar actividades laborales deberán suscribir un contrato de comodato o vale de resguardo con el IMDUyV, mediante el cual se autoriza que la persona encargada de Innovación acceda mensualmente al equipo para realizar los respaldos correspondientes y verificar la integridad de la información institucional generada.
El uso de equipos personales no exime al servidor público del cumplimiento de las obligaciones establecidas en los presentes Lineamientos.

CAPÍTULO III.
DE LOS ACTIVOS INFORMÁTICOS.

Articulo 11. Todo servidor público adscrito al IMDUyV que tenga asignado un activo informático para el desempeño de sus funciones será el único responsable de su uso, operación y de la información contenida en dicho equipo.
El servidor público deberá abstenerse de compartir o prestar el activo informático asignado. Únicamente podrá permitirse su utilización por otra persona para fines estrictamente laborales y previa autorización expresa de su superior jerárquico.

Articulo 12. La movilización de cualquier activo informático dentro o fuera de las instalaciones del IMDUyV será responsabilidad exclusiva del servidor público que tenga dicho equipo bajo su resguardo. Cuando el activo informático deba ser trasladado, el servidor público deberá informar por escrito a su superior jerárquico y a la persona encargada de Innovación, especificando el motivo, destino, fecha y hora del movimiento.
El traslado deberá realizarse utilizando las medidas necesarias para evitar daños, pérdida o acceso indebido a la información contenida en el equipo.

CAPÍTULO IV.
INTERCAMBIO DE INFORMACIÓN.

Artículo 13. Todo servidor público adscrito al IMDUyV que deba intercambiar información reservada o confidencial con personal interno o con terceros deberá verificar la identidad y personalidad de la persona receptora antes de entregar dicha información. El intercambio podrá realizarse por medios físicos o electrónicos y deberá contar con la autorización previa del superior jerárquico competente, asegurándose siempre que se apliquen las medidas de protección correspondientes a la clasificación de la información.

Artículo 14. Todo convenio o instrumento jurídico mediante el cual el IMDUyV comparta información reservada o confidencial con terceros deberá sujetarse estrictamente a las disposiciones aplicables en materia de acceso a la información pública, transparencia y protección de datos personales.
El convenio deberá establecer de manera expresa las obligaciones de confidencialidad, uso limitado, resguardo y las responsabilidades derivadas del manejo indebido de la información.

CAPÍTULO V.
DE LA PRESTACIÓN DE SERVICIOS POR TERCEROS.

Articulo 15. Todo proveedor que preste servicios informáticos al IMDUyV y que, para el cumplimiento de dichos servicios, tenga acceso a información reservada o confidencial, deberá observar en todo momento las disposiciones legales, reglamentarias y normativas aplicables en materia de acceso a la información pública y protección de datos personales. Además, deberá firmar y cumplir los acuerdos de confidencialidad y no divulgación necesarios para garantizar que la información no sea utilizada o revelada en perjuicio del Instituto.

Articulo 16. Todo servicio informático proporcionado por terceros deberá ser monitoreado y revisado por la persona responsable de su contratación y por la persona encargada de Innovación, a fin de verificar el cumplimiento de los términos, condiciones y obligaciones establecidas en los contratos, convenios o acuerdos correspondientes.
Cualquier incidencia, incumplimiento o riesgo detectado deberá documentarse y notificarse a la Dirección General para que determine las acciones procedentes.

CAPÍTULO VI.
PROTECCIÓN CONTRA CÓDIGO MALICIOSO (VIRUS Y MALWARE).

Articulo 17. Todo equipo de cómputo del IMDUyV deberá contar con un software antivirus y antimalware autorizado por la Dirección General y administrado por la persona encargada de Innovación.
En caso de que el software instalado no proporcione el nivel de protección requerido, el servidor público deberá notificar de inmediato a su superior jerárquico y a la persona encargada de Innovación, a fin de que se evalúe y determine la alternativa de solución más adecuada.

Articulo 18. Cualquier usuario que detecte anomalías, virus, actividad sospechosa, programas desconocidos o código malicioso en su equipo de cómputo deberá reportarlo de inmediato, en primer término, a su superior jerárquico y, posteriormente, a la persona encargada de Innovación del IMDUyV para su análisis, contención y solución inmediata.
El reporte oportuno será obligatorio para prevenir la propagación de riesgos que comprometan la integridad de la información institucional o la operación de los sistemas.

CAPÍTULO VII.
SERVICIOS INFORMÁTICOS EN LA RED.

Articulo 19. Todo servidor público adscrito al IMDUyV, así como pasantes o terceros que tengan acceso autorizado a los servicios informáticos institucionales, serán responsables del uso adecuado de dichos recursos, tanto dentro de las instalaciones como en plataformas alojadas en la nube. El uso de los servicios deberá realizarse exclusivamente para fines institucionales y en apego a los presentes Lineamientos.

Articulo 20. La persona encargada de Innovación será la única persona facultada para acceder a los equipos de cómputo del IMDUyV con el fin de realizar actividades técnicas, siempre previa autorización del superior jerárquico correspondiente o de la Dirección General.

Dichas actividades comprenden:

- Ejecutar las tareas derivadas del mantenimiento preventivo y correctivo.
- Realizar instalaciones, configuraciones o modificaciones del sistema operativo de los equipos de cómputo.
- Realizar revisiones de seguridad informática, diagnosticar incidentes y descartar daños a la información o al hardware.
- Instalar software y herramientas tecnológicas necesarias para el desempeño de actividades laborales.
- Sistema de gestión de datos de red

La persona encargada de Innovación deberá documentar las intervenciones realizadas y asegurar la integridad de la información contenida en los equipos.

Articulo 21. Las personas titulares de área o coordinaciones serán responsables de autorizar el acceso a los equipos de cómputo asignados a su personal, exclusivamente para fines relacionados con el ejercicio de las funciones institucionales.
Dicha autorización deberá otorgarse de forma controlada, salvaguardando la información contenida en los equipos.

Articulo 22. Ningún servidor público podrá copiar, alterar, eliminar o destruir la información almacenada en los equipos de cómputo o servidores institucionales sin el consentimiento expreso del responsable del equipo o del superior jerárquico competente. Cualquier acceso no autorizado constituirá una falta administrativa y podrá derivar en responsabilidades conforme a la Ley General de Responsabilidades Administrativas y la Ley de Responsabilidades Administrativas del Estado de Hidalgo.

Articulo 23. Todo servidor público que renuncie, sea separado de su cargo o sea reubicado a otra unidad administrativa, deberá presentar, como parte del acta de entrega-recepción, un listado completo de la información contenida en el equipo de cómputo bajo su resguardo. La información será revisada por la persona titular del área y deberá contar con la validación de la Dirección General. Una vez autorizada, la información deberá remitirse de manera inmediata a la persona encargada de Innovación, quien será responsable de su resguardo, preservación y protección conforme a la normativa aplicable.

Articulo 24. Todas las cuentas de usuario y sus respectivas contraseñas de acceso a los sistemas, plataformas y servicios informáticos del IMDUyV son personales e intransferibles.

Su uso será responsabilidad exclusiva del titular de la cuenta, únicamente durante la vigencia de los derechos y autorizaciones conferidas para el desempeño de sus funciones.
La creación, habilitación, modificación, suspensión o cancelación de las cuentas de usuario será facultad de la persona encargada de Innovación, conforme a las necesidades operativas del Instituto y a las solicitudes debidamente justificadas por las personas directivas o titulares de área.

Articulo 25. Los equipos de cómputo asignados al personal del IMDUyV incluyendo computadoras de escritorio, computadoras portátiles, impresoras y cualquier otro dispositivo conectado a la red institucional serán configurados exclusivamente por la persona encargada de Innovación, quien garantizará la correcta operación, protección y seguridad de la infraestructura tecnológica. Ningún servidor público ni persona ajena al área podrá modificar configuraciones técnicas, software, parámetros de red o mecanismos de seguridad de los equipos institucionales. En caso de fallas, pérdida de conectividad, errores de acceso o cualquier anomalía, el servidor público deberá reportarlo a la persona encargada de Innovación para su atención y solución.

Artículo 26. A toda persona que deje de laborar, concluya su relación profesional o sea reubicada dentro del IMDUyV, le será cancelado de manera definitiva cualquier acceso a los recursos informáticos institucionales. La persona titular del área correspondiente deberá comunicar por escrito a la persona encargada de Innovación toda alta, baja o cambio de adscripción del personal, para que éste adopte las medidas necesarias respecto de los privilegios de acceso, cuentas de usuario y permisos asociados a los servicios de red y sistemas institucionales.

CAPÍTULO VIII.
USO DE INTERNET.

Articulo 27. El servicio de Internet proporcionado a través de las redes institucionales del IMDUyV constituye una herramienta de trabajo y deberá ser utilizado por servidores públicos, estudiantes o terceros autorizados exclusivamente para actividades relacionadas con el cumplimiento de las funciones administrativas, técnicas o académicas que desempeñen.
Queda prohibido su uso para fines personales, recreativos o cualquier actividad ajena a los objetivos institucionales.

Articulo 28. Las personas titulares de área o coordinaciones podrán solicitar a la persona encargada de Innovación la restricción total o parcial del acceso a Internet del personal a su cargo, tomando en consideración las funciones que dicho personal realiza y la necesidad operativa de sus actividades. Las restricciones deberán aplicarse de manera proporcional y documentada.

Articulo 29. Todo servidor público del IMDUyV con acceso al servicio de Internet deberá abstenerse de descargar archivos, programas o información de sitios o fuentes de dudosa procedencia, ya que estos pueden contener virus, malware o software malicioso que comprometa la seguridad del equipo de cómputo, de la red institucional o de la información del IMDUyV. Las descargas deberán realizarse únicamente desde portales confiables, institucionales o autorizados por la persona encargada de Innovación.

CAPÍTULO IX.
CONTINUIDAD DE LAS OPERACIONES EN CASO DE DESASTRE.

Artículo 30. Para garantizar la continuidad operativa del IMDUyV en caso de desastres, siniestros o incidentes que afecten la infraestructura tecnológica, se establecen los siguientes procedimientos:

I. Los servidores públicos adscritos al IMDUyV deberán utilizar los procedimientos autorizados para la realización de copias de seguridad de los servicios informáticos y de la información generada en el ejercicio de sus funciones.
II. El Instituto contará con servidores de aplicaciones y bases de datos destinados al almacenamiento, respaldo y operación de los sistemas institucionales.
III. La persona encargada de Innovación recabará mensualmente la información digital correspondiente a cada unidad administrativa y generará un respaldo en un medio de almacenamiento externo autorizado. Dicho respaldo constituye una copia adicional y segura para mitigar los riesgos derivados de daños, pérdidas o destrucción de hardware, software o sistemas locales.
IV. Los medios utilizados para almacenar las copias de seguridad serán resguardados en una caja de seguridad ubicada en la oficina de la persona encargada de Innovación o en el área designada para tal efecto, garantizando su integridad, confidencialidad y disponibilidad.

Articulo 31. Para garantizar la continuidad de las operaciones del IMDUyV ante incendios, fallas mayores, catástrofes naturales o cualquier siniestro que afecte la infraestructura tecnológica, se deberá implementar el Plan de Recuperación de Desastres (PRD), el cual contempla los elementos y acciones siguientes:

I. Activación del plan y comunicación de la emergencia

1. Reportar de inmediato el siniestro a los números oficiales de emergencia.

2. Notificar a la Coordinación de Administración.
3. Informar al titular del área afectada y a la persona encargada de Innovación.
4. Alejarse de la zona de riesgo y seguir las instrucciones del personal responsable de seguridad.
5. Notificar a los usuarios la interrupción temporal de los servicios informáticos.

II. Acciones iniciales de protección y aseguramiento

1. Establecer un sitio de trabajo alterno para continuar actividades críticas.
2. Identificar y proporcionar el equipo mínimo indispensable para operar.
3. Conformar y organizar el equipo institucional de recuperación ante desastres.
4. Determinar el grado y alcance del siniestro.
5. Supervisar las condiciones de seguridad antes de iniciar cualquier operación técnica.

III. Recuperación de infraestructura y equipos

1. La persona encargada de Innovación ejecutará los procedimientos necesarios para la restauración del sistema de procesamiento de datos.
2. Reemplazar el equipo de cómputo dañado para los servidores públicos afectados.
3. Identificar el número de estaciones de trabajo necesarias para reanudar operaciones.
4. Comprobar los requerimientos técnicos de cada equipo conforme a las necesidades de cada área.
5. Preparar los equipos e instalar los programas necesarios para el funcionamiento laboral.
6. Planificar y gestionar el transporte seguro de los equipos y materiales necesarios hacia el sitio alterno o de respaldo.

IV. Restauración de información y sistemas

1. Facilitar las copias de seguridad a los titulares o directores de cada área administrativa.
2. Contactar y verificar la integridad de la base de datos proveniente del respaldo.
3. Implementar el plan de recuperación de la información según el nivel de daño identificado.
4. Establecer las planificaciones necesarias para la restauración total o parcial de los sistemas.
5. Verificar mediante formularios y registros que la información respaldada fue restaurada correctamente en los equipos asignados.

V. Registro, control documental y verificación

1. Llenar la bitácora de servicio correspondiente, con firma del Coordinador de Adquisiciones y Recursos Materiales y del servidor público que recibió el equipo restaurado.
2. Supervisar todas las fases del proceso de recuperación hasta su conclusión.
3. Seguir las listas de verificación establecidas en el PRD.
4. Mantener un listado actualizado del personal y sus números de contacto para la coordinación en caso de futuros incidentes.
5. Documentar las necesidades de suministros de oficina para garantizar la operación del sitio de contingencia.
6. Asegurarse de que cada servidor público conozca la información, actividades y funciones mínimas necesarias para reactivar los procesos de su área.

CAPÍTULO X
DE LOS EQUIPOS DE SOPORTE ELÉCTRICO.

Articulo 32. La persona encargada de Innovación será responsable de asegurar que cada equipo de cómputo del IMDUyV cuente con un regulador y un sistema de respaldo de voltaje (No-Break), con el fin de proteger su operación ante cortes de energía, variaciones eléctricas o sobrecargas.

Asimismo, la persona encargada de Innovación verificará, al menos de manera trimestral, el correcto funcionamiento de dichos dispositivos en las unidades administrativas, realizando los registros o reportes correspondientes para garantizar la continuidad operativa de los servicios informáticos.

CAPÍTULO XI.
DE LA ADQUISICIÓN DE BIENES INFORMÁTICOS.

Articulo 33. Toda adquisición de tecnología informática del IMDUyV deberá ser gestionada a través de la persona encargada de Innovación y contar con la autorización previa de la Dirección de Finanzas y Administración y de la persona titular de la Dirección General del Instituto.
Ninguna adquisición podrá llevarse a cabo sin cumplir con estos requisitos.

Artículo 34. La adquisición de bienes informáticos en el IMDUyV deberá sujetarse estrictamente a lo dispuesto en los presentes Lineamientos, así como a la normatividad aplicable en materia de adquisiciones, recursos materiales y disciplina financiera.

Artículo 35. La persona encargada de Innovación, al planear y gestionar las operaciones relacionadas con la adquisición de bienes informáticos, deberá establecer prioridades institucionales y considerar los siguientes criterios técnicos y operativos:

I. Estudio técnico o evaluación de necesidades.
II. Costo total y disponibilidad presupuestal.
III. Calidad y vida útil estimada.
IV. Capacidad y desempeño del equipo o solución.
V. Experiencia y solvencia del proveedor.
VI. Nivel de desarrollo tecnológico e innovación.
VII. Cumplimiento de estándares técnicos y de seguridad.
VIII. Impacto positivo en los procesos administrativos, recaudación o atención al público.

La adquisición deberá justificarse con base en estos criterios y documentarse en el expediente correspondiente.

Articulo 36. Para la adquisición de hardware en el IMDUyV deberán observarse los criterios siguientes:

I. El equipo a adquirir deberá contar con las características, capacidades y estándares necesarios para el cumplimiento eficiente de las actividades laborales del Instituto.
II. Todo equipo deberá contar, al menos, con un año de garantía por parte del proveedor o fabricante.
III. Los equipos deberán ser integrados de fábrica o, en su caso, ensamblados con componentes evaluados, verificados y aprobados por la persona encargada de Innovación, garantizando su compatibilidad y desempeño.
IV. Los dispositivos de almacenamiento y las interfaces de entrada y salida deberán cumplir con la tecnología vigente en términos de velocidad de transferencia, ciclos de procesamiento y estándares de conectividad, evitando adquisiciones obsoletas o incompatibles.
V. Las impresoras deberán apegarse a los estándares de hardware y software del mercado y del IMDUyV, asegurando que sus consumibles (tóner, tinta, papel u otros) sean fácilmente adquiribles y no dependan de un proveedor único.
VI. Todo proyecto relacionado con la adquisición de bienes informáticos deberá someterse al análisis, evaluación técnica, aprobación y autorización de la persona encargada de Innovación, antes de gestionarse ante las áreas competentes de finanzas y administración.

CAPÍTULO XII.
SEGURIDAD INFORMÁTICA.

Artículo 37. La persona encargada de Innovación del IMDUyV será responsable de la operación, administración y seguridad de la infraestructura tecnológica del Instituto. Para tal efecto, tendrá las atribuciones siguientes:

I. Brindar soporte técnico continuo a todas las unidades administrativas del IMDUyV. Realizar la reparación de equipos de cómputo institucionales.

II. Ejecutar los mantenimientos preventivos y correctivos conforme al programa autorizado.

III. Elaborar las bitácoras, registros y reportes derivados de las órdenes de servicio y actividades técnicas realizadas.

IV. Proporcionar asesoría técnica sobre el uso adecuado de programas, aplicaciones y sistemas informáticos.

V. Implementar proyectos tecnológicos, soluciones informáticas y ajustes necesarios en la infraestructura institucional.

VI. Gestionar la solicitud de consumibles, refacciones, equipos de cómputo y servicios relacionados, incluyendo su facturación.

VII. Llevar a cabo la entrega controlada de equipos, consumibles y materiales tecnológicos.

VIII. Atender, analizar y resolver los reportes relacionados con riesgos, fallas, vulnerabilidades o incidentes de seguridad informática.

IX. Asegurar el cumplimiento de las políticas, procedimientos y medidas establecidas en los presentes Lineamientos.

Articulo 38. Las políticas de seguridad informática del IMDUyV deberán implementarse, supervisarse y revisarse periódicamente por la persona encargada de Innovación, a fin de identificar la necesidad de ajustes, actualizaciones o nuevas medidas que permitan mitigar riesgos, fortalecer la protección institucional y garantizar el cumplimiento de la normativa vigente.

Para ello, deberán observarse, entre otras, las políticas siguientes:

a) Instalación, actualización y supervisión del antivirus institucional en todos los equipos de cómputo.

b) Configuración segura y uso responsable del correo electrónico institucional.

c) Control del inicio de sesión en equipos de cómputo mediante credenciales seguras.

d) Gestión del acceso y uso adecuado del servicio de Internet institucional.

e) Administración del acceso a la red local e infraestructura del IMDUyV.

f) Protección, manejo adecuado y renovación periódica de contraseñas.
g) Administración, actualización y configuración segura de los sistemas operativos.
h) Control de la conexión a redes inalámbricas autorizadas.
i) Control de acceso a sistemas, aplicaciones y plataformas institucionales.
j) Gestión y respaldo de bases de datos e información institucional.
k) Control de inventarios de equipos de cómputo y control de inventarios de impresoras y dispositivos periféricos, el cual debe solicitar a la dirección de Finanzas y Administración
l) Protección de la información institucional conforme a su clasificación.
m) Seguridad y resguardo adecuado de medios físicos de almacenamiento.

Artículo 39. Con el propósito de reducir riesgos y proteger la información institucional del IMDUyV, deberán implementarse medidas de seguridad orientadas a prevenir, mitigar y corregir incidentes que puedan ocasionar daños, pérdidas o accesos no autorizados. Para tal efecto, se observará lo siguiente:

a) Medidas preventivas: Acciones destinadas a anticipar y evitar vulnerabilidades, amenazas informáticas, intrusiones, ataques de hackers o cualquier riesgo potencial que comprometa la seguridad de los sistemas, redes o información institucional. Su implementación deberá incluir mecanismos de vigilancia, actualización, capacitación y control.
b) Medidas correctivas: Acciones orientadas a corregir fallas, brechas de seguridad o incidentes derivados de amenazas o ataques informáticos. Estas medidas deberán ejecutarse de manera inmediata para restaurar la operación normal, minimizar afectaciones y asegurar la integridad y disponibilidad de la información.
c) Riesgos asumibles: Aquellas vulnerabilidades no críticas cuyo potencial impacto sea limitado, cuyas probabilidades de explotación sean bajas o cuya atención inmediata no resulte prioritaria. Estos riesgos deberán ser identificados, monitoreados y gestionados mediante soluciones oportunas, procurando su mitigación progresiva conforme a la estrategia institucional de seguridad informática.

CAPÍTULO XIII
DE LAS VÍDEOGRABACIONES

Artículo 40. Las videograbaciones tienen por objeto captar, visualizar y monitorear de forma permanente imágenes del interior y exterior del IMDUyV que contribuyan a garantizar la

seguridad institucional, la prevención de riesgos, así como la identificación, documentación y persecución de hechos posiblemente constitutivos de delito o faltas administrativas.

Artículo 41. Para asegurar el correcto funcionamiento del sistema de videograbaciones, la persona encargada de Innovación será responsable de:

I. Monitorear quincenalmente las cámaras de videovigilancia para verificar su operatividad.
II. Verificar quincenalmente el estado y funcionamiento del disco duro u otro medio donde se almacenen las videograbaciones.

Articulo 42. El acceso a las videograbaciones será exclusivo de la persona encargada de Innovación y del titular de la Dirección General del IMDUyV. Ninguna otra persona podrá consultar o manipular dicho material sin autorización expresa por escrito de la Dirección General.

Articulo 43. Toda persona que, por motivo del ejercicio de sus funciones, tenga acceso al material videograbado, deberá mantener absoluta reserva, confidencialidad y discreción respecto de su contenido, absteniéndose de divulgarlo o utilizarlo para fines distintos a los institucionales.

Articulo 44. Cuando se requiera el material videograbado para esclarecer hechos presuntamente constitutivos de uno o varios delitos, faltas administrativas o investigaciones oficiales, la autoridad correspondiente deberá solicitarlo mediante oficio formal, debidamente autorizado por la persona titular de la Dirección General del IMDUyV.

Articulo 45. La persona encargada de Innovación entregará las videograbaciones solicitadas mediante memoria USB (preferentemente nueva) o disco duro externo, según el volumen del material, siempre previa autorización de la persona titular de la Dirección General del IMDUyV.

Articulo 46. La persona encargada de Innovación deberá verificar y validar que el contenido de las videograbaciones no contravenga la moral, los derechos de imagen, la legislación aplicable, ni las disposiciones en materia de protección de datos personales.

Articulo 47. Las videograbaciones deberán destruirse en su totalidad dentro de un plazo máximo de tres meses a partir de su captación, salvo que:

a) Estén relacionadas con un delito o una infracción administrativa.
b) Formen parte de una investigación policial, judicial o administrativa en curso.
c) Integren un expediente o procedimiento derivado del incumplimiento de los presentes Lineamientos.

En dichos casos, deberán conservarse hasta la conclusión del procedimiento correspondiente.

Articulo 48. Las instalaciones fijas de videocámaras, sistemas análogos y cualquier medio de videograbación tienen como finalidad proteger y garantizar la seguridad de los servidores públicos del IMDUyV, de los bienes muebles e inmuebles del Instituto y de la ciudadanía en general.

Articulo 49. En todas las instalaciones del IMDUyV deberán colocarse avisos visibles que informen a los servidores públicos y a la ciudadanía sobre la existencia de sistemas de videograbación y su finalidad.

CAPÍTULO XIV
DEL ÓRGANO INTERNO DE CONTROL

Articulo 50. La omisión o el incumplimiento de lo establecido en los presentes Lineamientos constituirá una falta administrativa no grave, de conformidad con lo dispuesto en el artículo 48 de la Ley de Responsabilidades Administrativas del Estado de Hidalgo, sin perjuicio de las demás sanciones o responsabilidades que pudieran derivarse conforme a la normativa aplicable.

Articulo 51. El Órgano Interno de Control del IMDUyV estará facultado para iniciar, de oficio o a petición de parte, la investigación correspondiente ante presuntos incumplimientos de los presentes Lineamientos, tanto por parte de los servidores públicos como de personas externas que interactúen con el Instituto. Dicha actuación se realizará conforme a lo establecido en la Ley de Responsabilidades Administrativas del Estado de Hidalgo y la normativa aplicable.

Artículo 55. Los servidores públicos y titulares de área deberán atender, en los plazos establecidos, toda solicitud de información, documentación, entrevistas, aclaraciones

o requerimientos que emita el Órgano Interno de Control con motivo de una supervisión, investigación o actuación derivada de estos Lineamientos.

Artículo 52. El Órgano Interno de Control podrá emitir recomendaciones, observaciones o medidas correctivas a las áreas del Instituto, cuando detecte riesgos, debilidades de control interno, incumplimientos, omisiones o cualquier situación que pudiera afectar la seguridad informática, el uso adecuado de los activos tecnológicos o la protección de datos personales.

Artículo 53. Los servidores públicos y titulares de área deberán atender, en los plazos establecidos, toda solicitud de información, documentación, entrevistas, aclaraciones o requerimientos que emita el Órgano Interno de Control con motivo de una supervisión, investigación o actuación derivada de estos Lineamientos.

Artículo 54. El Órgano Interno de Control, en coordinación con la persona encargada de Innovación, podrá solicitar la implementación de programas de capacitación obligatoria para los servidores públicos en temas de ética, uso responsable de recursos informáticos, protección de datos, seguridad digital y prevención de responsabilidades administrativas.

TRANSITORIOS

PRIMERO. Los presentes Lineamientos entrarán en vigor al día siguiente de su aprobación por la Junta de Gobierno del Instituto Municipal de Desarrollo Urbano y Vivienda, para conocimiento de todo el personal.

SEGUNDO. La persona encargada de Innovación, contará con un plazo máximo de treinta días hábiles a partir de la entrada en vigor de estos Lineamientos para realizar los ajustes técnicos, operativos y administrativos necesarios para su debido cumplimiento, incluyendo la actualización de sistemas, formatos, inventarios, procesos y mecanismos de control interno.

TERCERO. Los titulares de las unidades administrativas del IMDUyV deberán asegurar que el personal a su cargo sea informado y capacitado respecto del contenido y obligaciones derivadas de los presentes Lineamientos, en un plazo no mayor a treinta días hábiles contados a partir de su entrada en vigor, y deberán entregar informe de cumplimiento al Órgano Interno de Control.

Control de Cambios

No. de Revision	Fecha de Revision	Sección	Descripción y motivo del cambio
1	16/01/2025	Completo	Lineamientos de Uso, Administración y Seguridad de las Tecnologías de la Información y la Comunicación

ELABORÓ	REVISÓ	V.o.B.o.	AUTORIZO
L.D. MARCO ALEXIS MORENO CORREA	**L.D. ESTEFHANI ITZEL BARRERA RODRIGUEZ**	**MTRO. HIPÓLITO ZAMORA SORIA**	**ING. GRETCHEN ALYNE ATILANO MORENO**
AUTORIDAD RESOLUTORA DEL ORGANO INTERNO DE CONTROL DEL INSTITUTO MUNICIPAL DE DESARROLLO URBANO Y VIVIENDA.	TITULAR DEL ORGANO INTERNO DE CONTROL DEL INSTITUTO MUNICIPAL DE DESARROLLO URBANO Y VIVIENDA	DIRECTOR GENERAL DEL INSTITUTO MUNICIPAL DE DESARROLLO URBANO Y VIVIENDA	H. PRESIDENTA DE LA JUNTA DE GOBIERNO DEL INSTITUTO MUNICIPAL DE DESARROLLO URBANO Y VIVIENDA Y PRESIDENTA MUNICIPAL CONSTITUCIONAL DEL MUNICIPIO DE TIZAYUCA, HIDALGO

Expedición

Aprobación por Junta de Gobierno del Instituto Municipal de Desarrollo Urbano y Vivienda.

Sesión:	**Primera Sesión Extraordinaria del Ejercicio Fiscal 2026, de la Junta de Gobierno del Instituto Municipal de Desarrollo Urbano y Vivienda**
Acuerdo:	**IMDUYV/0030/JG/2026**
Fecha:	**20 DE ENERO DEL 2026**