ACUERDO IMDUYV/137/JG/23

LINEAMIENTOS PARA GARANTIZAR EL MANEJO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC´S) Y PROGRAMA DE SEGURIDAD INFORMATICA; AMBOS DEL INSTITUTO MUNICIPAL DE DESARROLLO URBANO Y VIVIENDA (IMDUYV).

ACUERDO QUE PROPONE LA PRESIDENCIA DE LA JUNTA DE GOBIERNO POR EL QUE SE APRUEBAN LOS LINEAMIENTOS PARA GARANTIZAR EL MANEJO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC´S) Y PROGRAMA DE SEGURIDAD INFORMATICA; AMBOS DEL INSTITUTO MUNICIPAL DE DESARROLLO URBANO Y VIVIENDA (IMDUYV).

M.A.P.P. Susana Araceli Ángeles Quezada, Presidenta Municipal Constitucional del Municipio de Tizayuca, Hidalgo y Presidenta Honorifica de la Junta de Gobierno como órgano máximo del Instituto Municipal de Desarrollo Urbano y Vivienda a la ciudadanía en general de conformidad con lo establecido en los artículos 115 de la Constitución Política de los Estados Unidos Mexicanos; y 85, 112 de la ley Orgánica Municipal del Estado de Hidalgo hace saber lo siguiente:

CONSIDERANDO

PRIMERO. Que el Instituto Municipal de Desarrollo Urbano y Vivienda, es un organismo público descentralizado de la administración pública municipal de Tizayuca, Hidalgo, con personalidad y patrimonio propio, así como autonomía técnica y de gestión para el cumplimiento de sus objetivos.

SEGUNDO. Mediante oficio número ASEH/DGFSM/120/OD-TIZ/2022 de fecha 01 de noviembre de 2023, emitido por el Auditor Superior del Estado

de Hidalgo, quien hizo del conocimiento al L.D. Jorge Luis Martínez Ángeles, Director General y la L.D. Orquídea Ortega Ortiz, Titular del Órgano Interno de Control, ambos de este Instituto, el informe de la cuenta pública del ejercicio fiscal 2022, a través del cual manifestó lo siguiente: *"la Entidad Fiscalizada carece de un documento o lineamientos con relación a los sistemas informáticos, donde se establezcan plan de recuperación y para dar continuidad a las operaciones en caso de desastre".* se observa que en el ejercicio fiscal 2022 no se contaba con dichos lineamientos.

TERCERO. Que este ente público está obligado a crear y mantener condiciones estructurales y normativas que permitan el adecuado funcionamiento del instituto para la actuación ética y responsable de cada servidor público, buscando acciones y creando normativa que regule el manejo y custodia de los sistemas informáticos con los que cuente este Instituto.

CUARTO. Por lo que la Dirección General, la Coordinación de Tecnologías y Sistemas de información y el Órgano Interno de Control, todos del Instituto Municipal de Desarrollo Urbano y Vivienda, coordinaron la elaboración de los presentes lineamientos, ello con la finalidad de atender las recomendaciones que realizó el ente fiscalizador antes señalado; con base en los principios de racionalidad, austeridad, disciplina, legalidad, honestidad, eficiencia, transparencia y objetividad, de conformidad con las disposiciones que en la materia establece, la Constitución Política de los Estados Unidos Mexicanos, la Ley General de Responsabilidades Administrativas, y demás normatividad aplicable.

Por lo anteriormente expuesto, tengo a bien, expedir el siguiente:

A C U E R D O.

LINEAMIENTOS PARA GARANTIZAR EL MANEJO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC´S) Y PROGRAMA DE SEGURIDAD INFORMATICA; AMBOS DEL INSTITUTO MUNICIPAL DE DESARROLLO URBANO Y VIVIENDA (IMDUYV).

CAPÍTULO I
DISPOSICIONES PRELIMINARES

ARTÍCULO 1.- Los Lineamientos de Seguridad Informática son diseñados y documentados para ser implementados en la adquisición, mantenimiento, soporte, desarrollo, uso y desecho de las tecnologías de la información del Instituto Municipal de Desarrollo Urbano y Vivienda (IMDUyV). Por lo cual su principal objetivo es garantizar, promover y preservar los recursos las TICS a través de medidas y formas eficientes que deben cumplir cabalmente la Coordinación de Tecnologías y Sistemas de Información 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 todos los Servidores Públicos del Instituto Municipal de Desarrollo Urbano y Vivienda (IMDUyV) que desempeñen labores o proporcionen algún tipo de servicio o producto y para la ciudadanía en general.

ARTÍCULO 3.- Los ordenamientos jurídicos administrativos vigentes que regulan la operación de las actividades tareas específicas para normar a

través de los lineamientos de seguridad informática, entre otros, son: la Constitución Políticas de los Estados Unidos Mexicanos; la Ley General de Transparencia y Acceso a la Información Pública; el Reglamento de Centro de Cómputo; la Ley de Responsabilidad de Servidores Públicos y la Ley General de Bienes Nacionales.

Artículo 4. Para efecto de los presentes lineamientos, se entenderá por:

Activo informático: Son recursos de sistemas informáticos que son necesarios para el desempeño de las funciones del usuario.

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

Comodato: Contrato por el cual se da o recibe prestada una cosa de las que pueden usarse sin destruirse, con la obligación de restituirla.

Equipo móvil: Es todo activo informático físico que tiene la facilidad de movilidad y que son necesarios para el desarrollo de las funciones de los colaboradores de este instituto, cómo laptops, tabletas, teléfonos inteligentes, entre otros.

IMDUyV: Instituto Municipal de Desarrollo Urbano y Vivienda.

Medio de almacenamiento removible: Medio externo al equipo de cómputo en el que se almacena información, como disquetes, CD, DVD, memorias (USB, SD, Otras), discos externos y resguardo en general.

OIC: Órgano Interno de Control.

Servicio informático: Bien intangible que se proporciona para satisfacer los requerimientos de los usuarios, relacionados con el uso del activo informático.

Software Institucional: Software con licenciamiento de uso y/o propietario que puede ser instalado y utilizado por los usuarios para el desempeño de sus actividades o funciones, o para la gestión de un servicio informático otorgado por este instituto.

Software libre: También conocido como freeware, shareware, Software demo, Software gratuito proveniente de internet o cualquier otro medio que no requiere la compra de una licencia para su uso.

TIC´S: Tecnologías de la Información y las Comunicaciones.

Usuario: Todo empleado o funcionario del instituto que haga uso de los activos o servicios informáticos de este organismo descentralizado, para el desempeño de sus funciones.

Virus: Programa informático creado para producir daño en el equipo o sistema.

Web, www. (World Wide Web): Es una convergencia de conceptos computacionales para presentar y enlazar información que se encuentra dispersa a través de internet de una forma fácilmente accesible.

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

Artículo 5. Es responsable de salvaguardar la información contenida en los equipos de cómputo de este instituto, el Coordinador de Tecnologías y Sistemas de Información y es quien efectuara respaldos de forma mensual; en base a un plan de trabajo y cronograma establecido.

Artículo 6. Es obligación de los servidores públicos adscritos al (IMDUyV) realizar respaldos de la información que se va generando diariamente a través de una organización de carpetas y de acuerdo a sus funciones establecidas.

Artículo 7. Todo servidor público adscrito al (IMDUyV) es responsable del resguardo de datos, debe confirmar que la información esté protegida para asegurar su integridad y confidencialidad, acorde a su clasificación. La información debe estar disponible de manera electrónica, impresa en papel, magnética, o bien, en algún otro medio.

Artículo 8. Todo servidor público adscrito al (IMDUyV) tendrá la obligación de hacer uso de la información a la que tenga acceso, únicamente para propósitos relacionados con el cumplimiento de cada una de sus funciones, debiendo resguardar forzosamente y principalmente los datos personales, absteniéndose de comunicarlos a terceros sin el consentimiento expreso de superior jerárquico.

Artículo 9. Todo servidor público adscrito al (IMDUyV) que hacen uso de información clasificada como restringida o confidencial, quedará bajo su responsabilidad la divulgación de los datos personales de conformidad con la LGRA y evitarán que sea accedida por personas no autorizadas.

Artículo 10. Para proteger la información contenida en los equipos de cómputo del (IMDUyV) todos los datos, archivos y documentos se encontrarán encriptados y contarán con contraseña; a la cual solo tendrán acceso la Coordinación de Tecnologías y Sistemas de Información y los servidores públicos adscritos a las Direcciones de Área.

Artículo 11. Los servidores públicos que utilicen sus equipos personales de cómputo realizarán un contrato de comodato con el (IMDUyV) para permitir mensualmente que el Coordinador de Tecnologías y Sistemas de Información pueda acceder libremente a respaldar la información generada de sus actividades laborales.

CAPÍTULO III.
DE LOS ACTIVOS INFORMÁTICOS.

Artículo 12. Todo servidor público adscrito al (IMDUyV) que tengan activo informático asignado de manera personal para uso de sus funciones son los únicos responsables de su utilización, así como la información contenida en los mismos, por lo que debe evitar compartirlos. En caso de requerir compartirlo o prestar el activo informático, será solamente para cuestiones laborales y previa autorización de su superior jerárquico.

Artículo 13. Toda movilización del activo informático dentro o fuera de las instalaciones de la institución es responsabilidad del Servidor Público resguardante y deberá informar por escrito a su superior jerárquico y al Coordinador de Tecnologías y Sistemas de información.

CAPÍTULO IV.
INTERCAMBIO DE INFORMACIÓN.

Artículo 14. Todo servidor público adscrito al (IMDUyV) que intercambie información reservada y/o confidencial con personal o terceras personas, debe asegurar la identidad y personalidad de la persona a la que le estregada la información, ya sea por medio físico o electrónico y previa autorización de su superior jerárquico.

Artículo 15. Todo convenio del (IMDUyV) con terceras personas para compartir 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.

CAPÍTULO V.
DE LA PRESTACIÓN DE SERVICIOS POR TERCEROS.

Artículo 16. Todo proveedor que proporcione servicios informáticos al (IMDUyV) y que tenga acceso a información reservada y/o confidencial, deberá apegarse a las disposiciones de las leyes, reglamentos y demás instrumentos normativos relacionado con acceso a la información pública y protección de datos personales y contar con acuerdos de no divulgación ni uso que perjudique al Instituto.

Artículo 17. Todo servicio informático otorgado por terceros deber ser monitoreado y revisado por la persona responsable de su contratación y por el Coordinador de Tecnologías y Sistemas de la información para asegurar que se cumplan con los términos estipulados en los acuerdos o contrato celebrado.

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

Artículo 18. Todo equipo de cómputo del (IMDUyV) debe contar con un Software Antivirus y Antimalware definido por la Dirección General y el Coordinador de Tecnologías y Sistemas de la Información. Si el software antivirus no cubre la protección necesaria, los servidores públicos notificarán a su superior jerárquico buscar una alternativa de solución.

Artículo 19. Todo usuario que identifique una anomalía, virus o software desconocido en su equipo de cómputo deberá reportarla (o) de inmediato en primer momento con su superior jerárquico y al Coordinador de Tecnologías y Sistemas de Información adscritos al (IMDUyV) para su inmediata solución.

CAPÍTULO VII.
SERVICIOS INFORMÁTICOS EN LA RED.

Artículo 20. Todo servidor público adscrito al (IMDUyV), estudiantes y terceros son responsables del buen uso de los servicios informáticos en cada una de las instalaciones y en la nube.

Artículo 21. Sólo el Coordinador de Tecnologías y Sistemas de Información queda facultado para acceder a los equipos de cómputo ubicados en el (IMDUyV) con finalidad de realizar, previa autorización de su superior jerárquico o en su de la Dirección General del Instituto lo siguiente:

- Ejecutar cada uno de las tareas del procedimiento de mantenimiento preventivo y correctivo.
- Realizar instalaciones y modificaciones del Sistema Operativo de cada uno de los equipos de cómputo.
- Realizar una revisión de seguridad informática y descartar cualquier daño a la información o hardware de cada uno de los equipos de cómputo.
- Realizar instalaciones de softwares necesarios para las actividades laborales en cada uno de los equipos de cómputo.

Artículo 22. Todo titular de área o departamento es responsable de autorizar el acceso al equipo de cómputo que tiene asignado, para que el personal a su cargo realice sus funciones.

Artículo 23. Ningún servidor público debe ver, copiar, alterar o destruir la información que reside en los equipos de cómputo y servidores sin el consentimiento explícito del responsable del equipo o de su superior jerárquico.

Artículo 24. Todo servidor público que renuncie, sea despedido o cambiado de área, hará a través de un acta entrega recepción un listado de la información contenida en su equipo de cómputo; la cual será revisada por el titular de su área y autorizada por la Dirección General. La información se remitirá de manera inmediata al Coordinador de Tecnologías y Sistemas de Información para su resguardo y protección.

Artículo 25. Todas las cuentas de usuario y su respectiva contraseña de acceso a los sistemas y servicios de información (IMDUyV), son personales, permitiéndose el uso bajo su responsabilidad, única y exclusivamente durante la vigencia de los derechos del usuario. La vigencia de las cuentas de usuarios es facultad Dirección de Tecnologías y Sistemas de Información, éstas son habilitadas, suspendidas o canceladas por el área en consideración a las necesidades o solicitudes realizadas por los directivos.

Artículo 26. El equipo de cómputo de cada uno de los servidores públicos adscritos al (IMDUyV) (computadoras de escritorio, computadoras portátiles e impresoras), será configurado solamente por el Coordinador de Tecnologías y Sistemas de Información para el resguardo y protección de la red. Todo servidor público o persona en general se abstendrá de realizar cambios en configuraciones de esta naturaleza, en caso de falla o error de acceso a internet.

Artículo 27. A toda persona que deje de laborar o tener relación con el (IMDUyV), le será cancelado su acceso de manera definitiva a los recursos informáticos institucionales. El Titular de su área comunicará al Coordinador de Tecnologías y Sistemas de Información toda alta, baja o cambio del personal para que se tomen las medidas correspondientes de privilegios de acceso a los servicios de red.

CAPÍTULO VIII.
USO DE INTERNET.

Artículo 28. El servicio de Internet a través de las redes institucionales se considera como herramienta de trabajo, por lo que todo servidor público, estudiante o tercero deberá utilizarlo exclusivamente para apoyo a las actividades administrativas que desempeñan.

Artículo 29. Todo responsable y titular de área 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.

Artículo 30. 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 IX.
CONTINUIDAD DE LAS OPERACIONES EN CASO DE DESASTRE.

Artículo 31. Procedimientos de Copia de Seguridad de Servicios Informáticos.

a) Los servidores públicos adscritos al (IMDUyV) utilizarán estos procedimientos para copia de seguridad de servicios informáticos.

b) Se contará con servidores de Aplicaciones y bases de datos.

c) Mensualmente el Coordinador de Tecnologías y Sistemas de Información recaudara el respaldo en un disco duro externo la información digital por unidad administrativa. De este modo se contará con una copia más segura de toda la información en caso de que un siniestro en el área local pudiera destruir hardware, software o sistemas.

d) Todos los medios se almacenarán en una caja de seguridad situada en la oficina del Coordinador de Sistemas de la Información.

Artículo 32. Plan de Recuperación de Desastres en Tics para su Continuidad

Para cualquier plan de recuperación en caso de siniestro, se deben tener en cuenta los siguientes elementos: Procedimientos de respuesta de emergencia para documentar la respuesta adecuada ante un incendio, una catástrofe natural o cualquier otro suceso similar, a fin de proteger a las personas y limitar los daños, por lo que se procederá a realizar lo siguiente:

I. Reportar a los teléfonos de emergencia.
II. Reportar a la Coordinación de Adquisiciones y Recursos Materiales.
III. Reportar al titular de área y al Coordinador de Tecnologías y Sistemas de la Información.
IV. Alejarse y estar pendiente de seguir las instrucciones del personal de la Dirección de Tecnologías para llevar a cabo las operaciones de copias de seguridad.
V. Establecer coordinadamente un sitio de trabajo alterno.

VI. Proporcionar el equipo mínimo para operar.

VII. El Coordinador de Adquisición y Recursos Materiales realizará procedimientos de acciones de recuperación para facilitar la restauración rápida de un sistema de proceso de datos.

VIII. Reemplazar el equipo de cómputo afectado a cada uno de los servidores públicos del instituto.

IX. Facilitar las copias de seguridad a los titulares o directores de cada área administrativa.

X. Preparar los equipos e instalar los programas necesarios para su funcionamiento laboral.

XI. Llenado de bitácora de servicio con firma del Coordinador de Adquisiciones y Recursos Materiales y del servidor público del instituto al que fue entregado el equipo de cómputo.

XII. Ponerse en contacto y organizar el equipo de recuperación en caso de siniestro.

XIII. Determinar el grado del siniestro.

XIV. Implementar el plan de recuperación de información en función de la amplitud del siniestro.

XV. Supervisar los procesos.

XVI. Contactar con la base de datos de la copia de seguridad y establecer planificaciones.

XVII. Notificar a los usuarios la interrupción del servicio.

XVIII. Seguir lista de comprobación.

XIX. Listar al personal y sus números de teléfono.

XX. Establecer el plan de participación de todos los usuarios.

XXI. Establecer suministros de oficinas de emergencia.

XXII. Identificar el número de estaciones de trabajo necesarias.

XXIII. Comprobar las necesidades de cada equipo de cómputo de conformidad con el área.

XXIV. Planificar el transporte de todos los elementos adicionales al local de copia de seguridad.

XXV. Comprobar los formularios necesarios para verificar que los datos de la copia de seguridad y la base de datos se trasladaron correctamente al equipo de cómputo correspondiente.

XXVI. Asegurarse que todos los servidores públicos del instituto conocen su información y actividades laborales.

CAPÍTULO X
DE LOS EQUIPOS DE SOPORTE ELÉCTRICO.

Artículo 33. El Coordinador de Tecnologías y Sistemas de Información se encargará que cada equipo de cómputo del (IMDUyV), contará con un regulador y respaldo de voltaje (No -break), con la finalidad de proteger su operación por cualquier corte de energía o sobrecarga eléctrica, también verificará quincenalmente que funcionen correctamente en las Unidades Administrativas del área financiera y Dirección General.

CAPÍTULO XI.
DE LA ADQUISICIÓN DE BIENES INFORMÁTICOS.

Artículo 34. Toda adquisición de tecnología informática se efectuará a través del Coordinador de Tecnologías y Sistemas de Información y debidamente autorizada por la Dirección de Finanzas, Administración y del Director General del (IMDUyV).

Artículo 35. La adquisición de bienes de informática en el (IMDUyV) quedará sujeta a los lineamientos establecidos en este documento.

Artículo 36. La Coordinación de Tecnologías y Sistemas de Información, al planear las operaciones relativas a la adquisición de bienes informáticos, establecerá prioridades y en su selección deberá tomar en cuenta: estudio técnico, precio, calidad, capacidad, experiencia, desarrollo tecnológico, estándares, impacto en la recaudación y/o atención al público.

Artículo 37. Para la adquisición de hardware se observará lo siguiente:

1) El equipo que se desee adquirir deberá contar con las características y los estándares requeridos para llevar a cabo las actividades laborales del (IMDUyV).

2) Deberán tener un año de garantía.
3) Deberán ser equipos integrados de fabrica o ensamblados con componentes evaluados por el Coordinador de Tecnologías y Sistemas de Información.

4) Los dispositivos de almacenamiento, así como las interfaces de entrada/salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos, cómo en el ciclo del proceso.

5) Las impresoras deberán apegarse a los estándares de Hardware y Software vigentes en el mercado y el (IMDUyV), corroborando con los suministros (tóner, papel, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.

6) Todo proyecto de bienes de informática, deberá sujetarse al análisis, aprobación y autorización del Coordinador de Tecnologías y Sistemas de la Información.

CAPÍTULO XII.
SEGURIDAD INFORMÁTICA.

1. RESPONSABILIDADES Y/O ATRIBUCIONES.

Artículo 38. A continuación, se tiene una descripción de las responsabilidades de la Coordinación de Tecnologías y Sistemas de Información del (IMDUyV).

I. Soporte técnico continuo.

II. Reparación de equipos de cómputo del (IMDUyV).
III. Ejecución de mantenimientos preventivos y correctivos.
IV. Elaboración de bitácoras o reportes relacionados con las órdenes de servicio.
V. Asesoría técnica respecto al uso de programas o sistemas.
VI. Implementación de nuevos proyectos, soluciones y/o ajustes en la infraestructura.
VII. Solicitud de consumibles y equipos de cómputo con proveedores. Facturación.
VIII. Entrega de consumibles y equipos.
IX. Solucionará los reportes de riesgo.

Artículo 39. Las políticas de seguridad informática deben ser implementadas y revisadas periódicamente, analizando la necesidad de cambios o adaptaciones para cubrir los riesgos existentes y verificar su cumplimiento.

a) Instalación de antivirus en cada uno de los equipos de cómputo del instituto;
b) Configuración y utilización de correo electrónico;
c) Logueo en equipos de cómputo;
d) Acceso a internet;
e) Acceso a la red;
f) Acceso y manejo adecuado de contraseñas;
g) Administración de sistemas operativos;
h) Conexión a redes inalámbricas;
i) Control de acceso a sistemas;
j) Control y manejo de base de datos y respaldo de información;
k) Control de inventario de equipos de cómputo;
l) Control de inventario de impresoras;
m) Seguridad de la información; y
n) seguridad de medios físicos.

Artículo 40. Con la finalidad de reducir el riesgo en el (IMDUyV) se deberán emplear las siguientes medidas para garantizar la seguridad de la información y así evitar daños y perdidas.

a) **Medidas preventivas:** Se deberán implementar para prevenir la posible vulnerabilidad por parte de una amenaza informática, hacker, etc.
b) **Medidas correctivas:** Se deberán implementar para corregir problemas o fallos de seguridad, debido a amenazas o ataques informáticos.
c) **Riesgos asumibles:** Se deberán confrontar todas aquellas vulnerabilidades que no sean sensibles y donde un riesgo las explote con rapidez, eficacia y soluciones.

CAPÍTULO XIII
DE LAS VÍDEOGRABACIONES

Artículo 41. El objeto de las vídeo grabaciones es captar, visualizar y monitorear de forma permanente dentro y fuera del (IMDUyV) toda imagen que contribuya a hacer efectiva su seguridad, prevención, persecución de hechos posiblemente constitutivos de delito y de las faltas administrativas.

Artículo 42. Para hacer efectivo el funcionamiento del sistema de vídeo grabaciones el Coordinador de Tecnologías y Sistemas de Información se encargará de:

I. Monitorear quincenalmente las cámaras para verificar su funcionamiento.
II. Verificar quincenalmente que el disco duro donde se almacenen las video grabaciones se encuentre funcionando correctamente.

Artículo 43. Solo tendrá acceso a las vídeo grabaciones el Coordinador de Tecnologías y Sistemas de Información y el Director General.

Artículo 44. Cualquier persona que por motivo del ejercicio de sus funciones tenga acceso a las grabaciones deberá observar en todo

momento la debida reserva, confidencialidad y discreción en relación a éstas.

Artículo 45. En caso de hechos posiblemente constitutivos de delito o faltas administrativas captadas por las cámaras, la autoridad correspondiente solicitará las vídeo grabaciones a través de oficio; el cual deberá ser autorizado por el Director General del (IMDUyV).

Artículo 46. Las vídeo grabaciones serán entregadas al solicitante por el Coordinador de Tecnologías y Sistemas de Información en memoria USB (De preferencia nueva) o Disco Duro según el espacio que ocupen las mismas; previa autorización del Director General del (IMDUyV).

Artículo 47. El Coordinador de Tecnologías y Sistemas de Información se encargará de verificar y validar que el contenido de las vídeo grabaciones no sea contrario a la moral ni a las leyes establecidas para la protección de la imagen de las personas.

Artículo 48. El Coordinador de Tecnologías y Sistemas de Información se encargará que las vídeo grabaciones sean destruidas en su totalidad dentro de un plazo máximo de cinco meses desde la fecha de su captación, salvo que estén relacionadas con la comisión de un delito, una infracción administrativa, una investigación policial en curso, un procedimiento judicial o administrativo o, en su caso, con cualquier hecho o conducta con el incumplimiento de los presentes lineamientos.

Artículo 49. Las instalaciones fijas de videocámaras o de cualquier otro medio análogo y, en general cualquier sistema que permita vídeo grabaciones tiene la finalidad de proteger y garantizar la seguridad de los servidores públicos del (IMDUyV), los bienes muebles e inmuebles del mismo y a la ciudadanía general.

Artículo 50. En las instalaciones del (IMDUyV) se colocarán letreros con avisos de grabación dirigidos a los servidores públicos y a la ciudadanía en general.

CAPÍTULO XIV
DEL ÓRGANO INTERNO DE CONTROL

Artículo 51. La omisión o incumplimiento de los presentes lineamientos constituirán falta administrativa no grave de conformidad con el artículo 49 de la Ley General de Responsabilidades Administrativas.

Artículo 52. El Órgano Interno de Control tendrá la facultad de iniciar la investigación correspondiente por presunto incumplimiento a los presentes lineamientos de los servidores públicos y ciudadanía general en el (IMDUyV) de conformidad con lo establecido por la Ley General de Responsabilidades Administrativas.

TRANSITORIOS

PRIMERO: El presente acuerdo entrará en vigor al día siguiente de su aprobación por Junta de Gobierno del Instituto Municipal de Desarrollo Urbano y Vivienda.

SEGUNDO: Se instruye a la Secretaría Técnica para que realice los trámites correspondientes para la publicación del presente acuerdo en la Gaceta Oficial Municipal de Tizayuca.

TERCERO: Se instruye a la Secretaría Técnica para que realice los trámites correspondientes para la publicación de los presentes lineamientos en la página web oficial del Instituto Municipal de Desarrollo Urbano y Vivienda https://imduyv.gob.mx/.

Dado en el domicilio legal del Instituto Municipal de Desarrollo Urbano y Vivienda, a los dieciséis días del mes de noviembre de dos mil veintitrés.

ASÍ LO APROBARON EN LA TRIGÉSIMA SESIÓN EXTRAORDINARIA DEL EJERCICIO FISCAL 2023 DE LA JUNTA DE GOBIERNO DEL INSTITUTO MUNICIPAL DE DESARROLLO URBANO Y VIVIENDA, POR UNANIMIDAD DE VOTOS LA PRESIDENTA MAESTRA SUSANA ARACELI ÁNGELES QUEZADA, ASÍ COMO LAS Y LOS INTEGRANTES DE LA JUNTA DE GOBIERNO DEL INSTITUTO MUNICIPAL DE DESARROLLO URBANO Y VIVIENDA, ARQUITECTA LAURA ADRIANA FONSECA RINCÓN, LICENCIADO EN CONTADURIA JUAN CARLOS MANZANO NIETO, LICENCIADO EN CIENCIAS POLÍTICAS Y ADMINISTRACIÓN PÚBLICA FERNANDO IRVING GARCIA SAMPERIO, CIUDADANO JAVIER ALAZAÑES SÁNCHEZ, INGENIERA GRETCHEN ALYNE ATILANO MORENO, INGENIERO HÉCTOR CHIMALPOPOCA ZAMBRANO Y EL LICENCIADO EN DERECHO JORGE LUIS MARTÍNEZ ÁNGELES EN SU CARÁCTER DE DIRECTOR GENERAL.

PRESIDENTA DE LA JUNTA DE GOBIERNO

M.A.P.P. Susana Araceli Ángeles Quezada

DIRECTOR GENERAL

L.D. Jorge Luis Martínez Ángeles