El suscrito Licenciado Gonzalo Esaú Cano Calvete, Secretario del Honorable Ayuntamiento del Municipio de Salamanca, Guanajuato, con fundamento en lo dispuesto en el artículo 137 fracción VI de la Ley para el Gobierno y Administración de los Municipios del Estado de Guanajuato, hago constar y certifico:

Que en la Trigésima Séptima Sesión Ordinaria celebrada el día dieciséis de abril del año dos mil veintiséis, el cuerpo edilicio tomó el siguiente:

ACUERDO: POR 14 (CATORCE) VOTOS A FAVOR Y 1 (UNO) EN CONTRA, SE APROBÓ EL DICTAMEN NÚMERO CU/HPCP/R/005/2024-2027, QUE FORMULAN LAS COMISIONES UNIDAS DE HACIENDA, PATRIMONIO Y CUENTA PÚBLICA; Y DE REGLAMENTOS; POR EL CUAL SE EXPIDEN LAS DISPOSICIONES ADMINISTRATIVAS EN MATERIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES PARA EL MUNICIPIO DE SALAMANCA, GUANAJUATO, para quedar en los siguientes términos:

DISPOSICIONES ADMINISTRATIVAS EN MATERIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES PARA EL MUNICIPIO DE SALAMANCA,GUANAJUATO

CAPÍTULO PRIMERO
DISPOSICIONES GENERALES

Naturaleza

Artículo 1. Las presentes Disposiciones Administrativas en materia de Tecnologías de la Información y Comunicaciones para el Municipio de Salamanca, Guanajuato son de carácter general y de observancia obligatoria para los servidores públicos que conforman la Administración Pública Municipal centralizada del Municipio de Salamanca, Guanajuato.

Objeto

Artículo 2. Las Disposiciones Administrativas en materia de Tecnologías de la Información y Comunicaciones para el Municipio de Salamanca, Guanajuato tendrán por objeto regular el uso de las tecnologías de la información y comunicaciones para el Municipio de Salamanca, Guanajuato, bajo un esquema de corresponsabilidad y uso en todas las actuaciones electrónicas entre los usuarios, áreas técnicas y administrativas, de tal forma que permitan el uso óptimo, racional y transparente, sin afectar la funcionalidad ni vulnerar la seguridad de la información que se procesa.

Glosario

Artículo 3. Para los efectos de las presentes Disposiciones Administrativa en materia de Tecnologías de la Información y Comunicaciones para el Municipio de Salamanca, Guanajuato, se entenderá por:

I. **Dependencias de la Administración Pública:** son las dependencias y unidades administrativas que conforman la estructura orgánica de la Administración Pública Municipal centralizada del Municipio de Salamanca, Guanajuato;

II. **Dictamen técnico:** es el documento oficial, con carácter vinculante o consultivo

según el caso, emitido por la Dirección de Tecnologías de Información, mediante el cual se evalúan, verifican y dictaminan aspectos técnicos, funcionales, de interoperabilidad, seguridad, arquitectura tecnológica, escalabilidad y alineación normativa de los sistemas de información, plataformas, bienes o servicios digitales que pretendan adquirirse, desarrollarse, implementarse o contratarse por el Municipio.

Dicho dictamen constituye un instrumento de control y validación previa, cuyo objeto es asegurar la compatibilidad tecnológica, la eficiencia operativa, la sostenibilidad presupuestal y el cumplimiento de los principios rectores en materia de gobierno digital, transparencia, protección de datos personales y administración pública digital establecidos en la normativa estatal y municipal;

III. **Dirección:** la Dirección de Tecnologías de la Información, adscrita a la Oficialía Mayor;

IV. **Disposiciones Administrativas:** son las Disposiciones Administrativas en materia de Tecnologías de la Información y Comunicaciones para el Municipio de Salamanca, Guanajuato;

V. **Hardware:** son todos los componentes físicos de servidores, computadoras, dispositivos de comunicación, equipos y periféricos;

VI. **Municipio:** el Municipio de Salamanca, Guanajuato;

VII. **Sistema de información:** es el conjunto organizado e interrelacionado de componentes tecnológicos, humanos y procedimentales, cuyo propósito es capturar, almacenar, procesar, administrar, proteger y distribuir información relevante para la toma de decisiones, prestación de servicios, cumplimiento de funciones públicas o ejercicio de atribuciones institucionales en el ámbito del Municipio;

VIII. **Software:** son los programas, aplicaciones y desarrollos asociados con la operación de un sistema; y,

IX. **Usuarios:** es toda aquella persona que hace uso de los sistemas, aplicaciones y de las tecnologías de información y comunicaciones.

Sujetos de aplicación

Artículo 4. Son sujetos de la aplicación de estas Disposiciones Administrativas, los usuarios de las Dependencias de la Administración Pública.

CAPÍTULO SEGUNDO
LOS SISTEMA DE INFORMACIÓN

Cumplimiento

Artículo 5. Los sistemas de información institucionales del Municipio deberán operar en estricta observancia a lo establecido en las presentes Disposiciones Administrativas, conforme a su objeto, naturaleza jurídica y el tipo de información

que resguarden, generen, procesen o administren. Su desarrollo, implementación y uso deberán alinearse con los principios rectores en materia de tecnologías de la información y comunicaciones, garantizando la interoperabilidad, seguridad, confidencialidad, disponibilidad y transparencia de la información pública, en apego a la normativa aplicable.

Dictamen técnico

Artículo 6. Todo sistema de información que se pretenda adquirir, desarrollar o contratar para el Municipio deberá contar, con carácter previo al inicio .del procedimiento correspondiente, con el dictamen técnico emitido por la Dirección.

Dicho dictamen técnico será requisito indispensable para la validación técnica de la solución propuesta y deberá integrarse, conforme al monto autorizado y al procedimiento de contratación aplicable, ya sea adjudicación directa, licitación restringida o licitación pública, al expediente de contratación respectivo.

Asimismo, deberá anexarse el formato de solicitud de bienes y servicios emitido por la Dirección de Recursos Materiales, o en su caso, el acuerdo correspondiente del Comité de Contrataciones Públicas del Municipio de Salamanca, Guanajuato, de conformidad con lo establecido en la normativa municipal aplicable.

Mecanismos técnicos y administrativos de seguridad

Artículo 7. Los sistemas de información deberán incorporar de manera obligatoria, mecanismos técnicos y administrativos de seguridad que aseguren la integridad, confidencialidad, disponibilidad y trazabilidad de la información.

Asimismo, deberán implementar controles de acceso diferenciados y gestionados conforme a perfiles de usuario previamente autorizados, en atención al nivel de consulta, uso o administración requerido, conforme a lo determinado por la Dirección, a propuesta fundada y motivada de las dependencias de la Administración Pública involucradas.

Dichos mecanismos deberán observar lo dispuesto en la normativa aplicable en materia de seguridad de la información, protección de datos personales, gobierno digital y control interno institucional.

Documentación obligatoria para sistemas de información

Artículo 8. Todo sistema de información desarrollado ya sea mediante recursos internos o a través de terceros, deberá entregarse debidamente documentado, con el fin de garantizar su correcta operación, mantenimiento, actualización, interoperabilidad y recuperación ante incidentes o desastres tecnológicos.

La Dirección deberá integrar y resguardar, como mínimo, la siguiente documentación técnica y administrativa que deberá ser proporcionada por el desarrollador o proveedor al momento de la entrega formal y/o puesta en operación del sistema, siendo la siguiente:

I. Solicitud de desarrollo de sistemas, debidamente firmada y requisitada, que deberá contener, lo siguiente:

a) Descripción clara del problema o situación a resolver;

b) Objetivo general del sistema;

c) Requerimientos funcionales y no funcionales del sistema;

d) Resultados esperados y métricas de desempeño; e,

e) Nombre y datos del enlace responsable designado por la dependencia de la Administración Pública solicitante, quien será el encargado de revisar, validar y dar visto bueno al sistema;

II. Memoria técnica, que deberá contener los elementos necesarios para garantizar la instalación, operación, mantenimiento y recuperación del sistema, incluyendo al menos lo siguiente:

a) Requerimientos técnicos de instalación;

b) Sistema operativo y versiones compatibles;

c) Especificación de bases de datos utilizadas;

d) Licenciamiento requerido;

e) Requerimientos mínimos de hardware; e,

f) Credenciales de acceso, siendo usuarios y contraseñas, en caso de ser necesarias para el entorno técnico;

III. Manual de usuario, en formato físico o electrónico, que describa las funcionalidades del sistema, procedimientos de uso y buenas prácticas operativas; y,

IV. Información del proveedor, en caso de que se trate de un sistema desarrollado externamente, incluyendo datos de contacto, mecanismos de soporte, canales de comunicación oficiales, y condiciones de garantía o mantenimiento.

Titularidad y derechos patrimoniales sobre los sistemas de información

Artículo 9. Los sistemas de información que sean desarrollados con recursos internos, contratados con terceros o adquiridos mediante cualquier modalidad legal por parte del Municipio, serán considerados bienes intangibles de dominio público, y en consecuencia, su titularidad corresponderá íntegramente al Municipio.

Esta titularidad comprende, sin excepción, los derechos patrimoniales sobre el código fuente, siendo en el caso de desarrollos a medida, licencias de uso,

distribución o reproducción, manuales, documentación técnica, modelos de datos, certificados digitales, mecanismos de seguridad asociados, así como cualquier otro componente necesario para el funcionamiento, administración, mantenimiento o modificación del sistema.

En los contratos con proveedores externos, deberá establecerse expresamente la cesión total de los derechos patrimoniales y de explotación a favor del Municipio, así como la entrega oportuna de todo elemento necesario para asegurar su soberanía tecnológica y autonomía operativa.

Aspectos contractuales mínimos para el desarrollo o adquisición de sistemas de información

Artículo 10. En toda contratación que implique el desarrollo, implementación, adquisición o suministro de sistemas de información por parte de terceros, el Municipio deberá prever expresamente en los términos contractuales, al menos, los siguientes aspectos esenciales:

I. Número y tipo de licencias de uso autorizadas, incluyendo su alcance territorial, temporal y condiciones de renovación, en su caso;

II. Límites de instalación y despliegue, especificando el número de equipos, servidores, ambientes de desarrollo, prueba y producción donde podrá instalarse la aplicación;

III. Derechos de modificación y adaptación del software, incluyendo condiciones para el acceso al código fuente, documentación y manuales técnicos;

IV. Servicios de soporte técnico y mantenimiento, especificando niveles de servicio, tiempos de respuesta y mecanismos de atención durante y después del periodo de implementación;

V. Cláusula de confidencialidad, protección de datos personales y tratamiento de la información institucional que sea accesada, generada o manipulada durante el desarrollo o ejecución del sistema o proyecto, conforme a la normativa aplicable; y,

VI. Garantías técnicas y legales aplicables, que aseguren la operatividad, seguridad y funcionalidad del sistema durante el periodo pactado, así como mecanismos de penalización en caso de incumplimiento.

Estos aspectos deberán ser revisados, validados y aprobados por la Dirección en coordinación con Dirección de Recursos Materiales, como condición previa para la formalización del contrato correspondiente.

Actualización, modificación y registro de sistemas de información

Artículo 11. Todo sistema de información desarrollado, contratado o adquirido por el Municipio deberá contar, desde su implementación, con la documentación completa que acredite la titularidad de la licencia de uso, así como cuando

proceda, el código fuente correspondiente, con el objeto de garantizar su actualización, adecuación, mejora continua o modificación conforme a los requerimientos funcionales y operativos de las dependencias municipales.

Dicha información deberá estar debidamente registrada y resguardada por la Dirección, en coordinación con la Dirección de Recursos Materiales, y será condición indispensable para asegurar la continuidad operativa, interoperabilidad, mantenimiento y evolución tecnológica del sistema.

La omisión de este requisito deberá ser observada como causal de improcedencia para la recepción o formalización del sistema de información, sin perjuicio de las responsabilidades administrativas o contractuales que correspondan.

CAPÍTULO TERCERO
USO, ADQUISICIÓN Y ASIGNACIÓN DE BIENES INFORMÁTICOS Y TECNOLÓGICOS

Autorización de adquisición, sustitución o arrendamiento de bienes informáticos y tecnológicos

Artículo 12. La Dirección propondrá a la Oficialía Mayor, por conducto de la Dirección de Recursos Materiales, la autorización para la adquisición, sustitución o arrendamiento de bienes informáticos y tecnológicos requeridos por las distintas dependencias de la Administración Pública, conforme a las necesidades operativas detectadas y dentro de los límites del ejercicio presupuestal autorizado.

La propuesta deberá incluir el número, tipo, especificaciones técnicas, vida útil estimada y justificación funcional de los equipos o bienes requeridos, observando en todo momento los criterios de eficiencia, sustentabilidad tecnológica, compatibilidad e interoperabilidad institucional, así como las disposiciones normativas vigentes en materia de adquisiciones y control patrimonial.

La Dirección será responsable de vigilar que las solicitudes se apeguen a los lineamientos de renovación, uso racional de recursos y criterios técnicos establecidos para la sustitución de equipo de cómputo y demás bienes tecnológicos.

Normatividad aplicable en la adquisición de bienes informáticos y tecnológicos

Artículo 13. La adquisición de bienes informáticos y tecnológicos por parte del Municipio, deberá realizarse en estricto apego a los Lineamientos Generales en Materia de Racionalidad, Austeridad y Disciplina Presupuestal del Municipio de Salamanca, Guanajuato para el ejercicio fiscal correspondiente, así como a las disposiciones jurídicas aplicables en materia de adquisiciones, arrendamientos y servicios del sector público.

En todo procedimiento de adquisición deberá privilegiarse el uso eficiente de los recursos públicos, la sustentabilidad tecnológica, la compatibilidad institucional y el cumplimiento de los objetivos operativos y estratégicos del Municipio, asegurando que los bienes adquiridos respondan a criterios técnicos

debidamente justificados, sin comprometer la disciplina financiera ni la transparencia administrativa.

Validación técnica previa a la adquisición de bienes informáticos y tecnológicos

Artículo 14. Todo bien informático o tecnológico cuya adquisición haya sido autorizada por la Dirección de Recursos Materiales o, en su caso, por el Comité de Contrataciones Públicas del Municipio de Salamanca, Guanajuato, deberá contar previamente con la validación técnica emitida por la Dirección.

Esta validación tendrá por objeto verificar que las características técnicas de los bienes propuestos se encuentren alineadas con los criterios de interoperabilidad, compatibilidad, eficiencia y sustentabilidad definidos en el Catálogo Institucional de Equipos de Cómputo autorizado por el Comité de Tecnologías de la Información del Municipio.

Ningún procedimiento de compra podrá formalizarse sin dicha validación técnica, la cual será requisito indispensable para garantizar la estandarización tecnológica y la correcta integración de los bienes al entorno digital institucional.

Uso institucional de bienes informáticos y tecnológicos

Artículo 15. Los bienes informáticos y tecnológicos asignados a servidores públicos del Municipio deberán ser utilizados única y exclusivamente para el ejercicio de las funciones inherentes a su cargo, conforme a las atribuciones y responsabilidades que les hayan sido conferidas por la normatividad vigente y las disposiciones administrativas aplicables.

Queda prohibido el uso de dichos bienes para fines personales, comerciales o ajenos al servicio público. Su utilización deberá sujetarse a criterios de racionalidad, eficiencia, seguridad de la información y observancia del marco jurídico aplicable en materia de tecnologías de la información, protección de datos personales y uso responsable de recursos públicos.

La Dirección podrá emitir lineamientos específicos para la gestión, control y monitoreo del uso de los equipos, a fin de prevenir usos indebidos y garantizar su disponibilidad y funcionalidad institucional.

Resguardo y traslado de bienes informáticos

Artículo 16. En los casos en que los bienes informáticos y tecnológicos del Municipio sean objeto de reubicación física entre distintas áreas de la Administración Pública o usuarios, el servidor público que tenga asignado el resguardo de dichos bienes será responsable de gestionar, con carácter previo al traslado, los trámites correspondientes ante la Dirección de Control Patrimonial, a efecto de actualizar los registros de inventario institucional.

Esta obligación tiene como finalidad garantizar la trazabilidad, integridad y control adecuado de los activos tecnológicos, conforme a las disposiciones normativas en materia de administración de bienes muebles y control patrimonial vigentes en

el Municipio.

El incumplimiento de esta disposición podrá derivar en responsabilidades administrativas conforme a la legislación aplicable.

CAPÍTULO CUARTO
ASIGNACIÓN Y USO DE TELEFONÍA FIJA Y EXTENSIONES TELEFÓNICAS

Uso institucional de servicios electrónicos y de telecomunicaciones

Artículo 17. El uso de los servicios electrónicos institucionales, incluyendo acceso a redes informáticas, servicios de comunicaciones digitales, telefonía fija y extensiones telefónicas asignadas a los servidores públicos del Municipio, deberá destinarse exclusivamente al cumplimiento de funciones oficiales y tareas inherentes al cargo que desempeñen.

Dichos servicios deberán utilizarse bajo un marco de corresponsabilidad, eficiencia, racionalidad y transparencia, conforme a los principios de legalidad y buen uso de los recursos públicos.

La Dirección podrá establecer políticas y mecanismos de supervisión, así como aquellos que regulen el uso responsable de dichos servicios, sin perjuicio de las responsabilidades administrativas que pudieran derivarse en caso de uso indebido o personal.

Autorización y titularidad en la contratación de servicios de telefonía fija

Artículo 18. La contratación de servicios de telefonía fija, así como la asignación de equipos y extensiones telefónicas, deberá ser autorizada por la Dirección, con base en los requerimientos técnicos, operativos y presupuestales debidamente justificados.

Los equipos, líneas y extensiones telefónicas que se adquieran o habiliten en virtud de dicha contratación serán considerados propiedad del Municipio, y deberán integrarse al inventario institucional correspondiente bajo los criterios de resguardo, uso responsable y control patrimonial.

La Dirección será responsable de emitir las especificaciones técnicas necesarias para garantizar la eficiencia, compatibilidad y adecuada funcionalidad del servicio en el entorno institucional.

Asignación de equipos y extensiones telefónicas

Artículo 19. La asignación de equipos y extensiones telefónicas a servidores públicos deberá ser autorizada por la Dirección, previa solicitud formal y debidamente justificada por parte de los titulares de las dependencias de la Administración Pública.

Dicha asignación deberá atender criterios de funcionalidad operativa, uso racional de recursos, jerarquía administrativa y disponibilidad presupuestal, y quedará sujeta a registro patrimonial.

El usuario asignado será responsable del uso correcto, conservación y resguardo de los equipos y extensiones, conforme a las disposiciones vigentes en materia de bienes muebles y recursos tecnológicos.

Cancelación y reubicación de servicios de telecomunicaciones

Artículo 20. Será responsabilidad directa del titular del área administrativa correspondiente notificar por escrito a la Dirección cualquier cancelación, suspensión temporal o reubicación de los servicios de telefonía fija o extensiones telefónicas previamente contratados o asignados.

En dichos casos, deberá gestionarse el reintegro inmediato a la Dirección de todos los equipos, dispositivos y accesorios vinculados al servicio en cuestión, a efecto de su registro, resguardo o reasignación conforme a los procedimientos establecidos.

Actualización de usuarios asignados a extensiones telefónicas

Artículo 21. Corresponde a los titulares de cada dependencia de la Administración Pública informar oportunamente a la Dirección cualquier cambio en la adscripción, reasignación o modificación del personal usuario de las extensiones telefónicas asignadas a su área administrativa.

Dicha notificación deberá realizarse de manera inmediata una vez efectuado el cambio, con el propósito de mantener actualizados los registros del conmutador institucional y el directorio telefónico oficial administrado por la Dirección de Recursos Humanos.

La falta de actualización de esta información podrá afectar la operatividad de los servicios de telecomunicaciones, y dará lugar a las observaciones administrativas que correspondan.

CAPITULO QUINTO
OBLIGACIONES Y RESPONSABILIDADES DE LOS USUARIOS

Responsabilidad de los usuarios en el manejo de información institucional

Artículo 22. En el ejerc1c10 de sus funciones y dentro del ámbito de sus competencias, los servidores públicos usuarios de los sistemas de información del Municipio serán responsables del ingreso, procesamiento, resguardo y uso

de los datos y registros administrados en dichos sistemas, así como de toda información alojada en los servidores institucionales, conforme a los principios de legalidad, seguridad, confidencialidad y uso responsable.

Cuando la información procesada o generada sea considerada como reservada, confidencial o sensible, en términos de la legislación en materia de transparencia y protección de datos personales, el usuario responsable deberá adoptar las medidas técnicas y administrativas necesarias para garantizar su resguardo y no divulgación, tales como el uso de contraseñas seguras, compresión de archivos, encriptación de información, o solicitud de respaldos periódicos ante la Dirección.

Notificación obligatoria de cambios o bajas de usuarios de sistemas institucionales

Artículo 23. Los titulares de las dependencias de la Administración Pública serán responsables de notificar de manera inmediata y por escrito a la Dirección cualquier cambio, reasignación o baja de los servidores públicos que cuenten con acceso autorizado a los sistemas de información institucionales.

Esta notificación tendrá como finalidad salvaguardar la integridad, disponibilidad y confidencialidad de la información, así como garantizar la correcta gestión de accesos, roles y privilegios dentro de los sistemas tecnológicos del Municipio.

Solicitud y autorización de accesos a sistemas institucionales

Artículo 24. Los titulares de las dependencias y unidades administrativas que integran la Administración Pública deberán solicitar formalmente a la Dirección la asignación de roles, perfiles y niveles de acceso a los sistemas institucionales para los servidores públicos bajo su responsabilidad.

Dicha solicitud deberá estar debidamente justificada en atención de las funciones, atribuciones y responsabilidades asignadas al colaborador, y será condición necesaria para autorizar el acceso a los sistemas, módulos o funcionalidades requeridas para el desempeño de sus actividades laborales.

La Dirección validará técnicamente la viabilidad de la asignación solicitada y será responsable de implementar los controles correspondientes para asegurar la trazabilidad, integridad y protección de la información.

Mantenimiento y configuración de bienes informáticos y tecnológicos

Artículo 25. Queda estrictamente prohibido a los usuarios de la Administración Pública realizar, por cuenta propia o a través de terceros no autorizados, actividades de mantenimiento preventivo o correctivo, configuración, instalación de software, modificación de parámetros técnicos, o cualquier otra intervención sobre los bienes informáticos y tecnológicos asignados.

Estas actividades únicamente podrán ser llevadas a cabo por el personal técnico expresamente autorizado por la Dirección, conforme a los protocolos establecidos para tal efecto.

El incumplimiento de esta disposición podrá derivar en la revocación de los accesos, la pérdida del equipo asignado o responsabilidades administrativas en términos de la normatividad aplicable.

Prohibiciones específicas para los usuarios de bienes y servicios informáticos

Artículo 26. Queda expresamente prohibido a los usuarios de bienes informáticos, tecnológicos y servicios electrónicos del Municipio realizar cualquiera de las conductas siguientes:

I. Instalar, ejecutar o permitir la instalación de software, aplicaciones, complementos o herramientas que no cuenten con la autorización previa y por escrito de la Dirección, en especial aquellos que puedan comprometer la estabilidad, seguridad o integridad de los sistemas;

II. Resguardar, respaldar o almacenar en los servidores, sistemas institucionales o dispositivos de almacenamiento oficial, archivos personales tales como documentos, imágenes, música, videos, juegos o cualquier otro contenido ajeno a las funciones laborales que le hayan sido asignadas;

III. Manipular físicamente los equipos de cómputo del Municipio, en particular insertar, remover o sustituir componentes internos tales como discos duros, módulos de memoria, tarjetas madre, de video, audio, redes u otros periféricos, sin autorización técnica de la Dirección;

IV. Realizar cualquier conducta que contravenga lo dispuesto en las presentes Disposiciones Administrativas, o que derive en el mal uso de los sistemas, servicios o equipos institucionales;

V. Ejecutar acciones que vulneren, interfieran o comprometan la confidencialidad, integridad o disponibilidad de la información procesada, resguardada o publicada en la intranet institucional, sistemas de gestión, portales oficiales, páginas web o servicios en línea del Municipio;

VI. Utilizar el servicio de internet institucional para descargar, almacenar o compartir archivos de música, películas, videojuegos, software no autorizado, contenido multimedia o cualquier otro material no relacionado con el desempeño de funciones oficiales; y,

VII. Acceder, consultar o interactuar con sitios web que contengan contenido pornográfico, juegos de azar, entretenimiento no laboral, apuestas en línea, redes de intercambio de archivos o cualquier otro portal que pueda poner en riesgo la reputación, seguridad o recursos tecnológicos del Municipio.

Uso autorizado de software y hardware

Artículo 27. Los usuarios únicamente podrán hacer uso del software, aplicaciones, periféricos y componentes de hardware que hayan sido previamente instalados, configurados o autorizados por el personal técnico designado por la Dirección.

Queda estrictamente prohibida la instalación, sustitución, modificación o utilización de cualquier software o componente de hardware no validado institucionalmente, aun cuando su uso tenga fines laborales, salvo autorización expresa por escrito de la Dirección.

Esta disposición tiene como finalidad garantizar la integridad, estabilidad, compatibilidad y seguridad del entorno tecnológico institucional, así como evitar riesgos operativos y legales derivados del uso de software no licenciado o hardware no certificado.

Procedimiento en caso de extravío, robo o daño intencional de bienes informáticos

Artículo 28. En caso de extravío, sustracción indebida, daño intencional o uso negligente que resulte en afectaciones al hardware, software o cualquier componente tecnológico propiedad del Municipio, el servidor público usuario deberá informar de inmediato a su superior jerárquico directo, quien a su vez estará obligado a notificar formalmente el incidente a la Dirección de Control Patrimonial.

Esta notificación tendrá como finalidad documentar el suceso, deslindar responsabilidades, activar los procedimientos de reposición, baja o responsabilidad patrimonial que correspondan, y proceder conforme a lo establecido en la normativa municipal aplicable en materia de bienes muebles, responsabilidades administrativas y control interno.

Lo anterior, sin perjuicio de las acciones civiles, administrativas o penales que puedan derivarse de la conducta del usuario en caso de dolo, culpa o negligencia grave.

Entrega y gestión de accesos a servicios electrónicos

Artículo 29. La Dirección será la encargada de generar y entregar a los servidores públicos los usuarios y accesos a los sistemas institucionales y servicios electrónicos previamente autorizados por los titulares de las dependencias o unidades administrativas, mediante la presentación del formato oficial de Entrega de Servicios Electrónicos.

La entrega de credenciales deberá realizarse de manera estrictamente personal y presencial, siendo responsabilidad del usuario realizar el cambio inmediato de la contraseña asignada, la cual será de uso exclusivo, confidencial e intransferible.

En caso de olvido, bloqueo o compromiso de las credenciales, el usuario podrá solicitar su reposición a la Dirección mediante los mecanismos establecidos, observando en todo momento los protocolos de seguridad y validación de identidad institucional.

Uso institucional de la cuenta de correo electrónico oficial

Artículo 30. La cuenta de correo electrónico institucional asignada a los servidores públicos del Municipio, deberá utilizarse exclusivamente para fines laborales, en el ejercicio de las funciones y atribuciones inherentes a su cargo.

El usuario será responsable del contenido, destino y gestión de la información que transmita, reciba o comparta a través de dicho medio, debiendo observar en todo momento los principios de legalidad, confidencialidad, profesionalismo y uso responsable de las comunicaciones oficiales.

Queda expresamente prohibido el uso del correo institucional para el envío de mensajes masivos, cadenas, publicidad, contenido no relacionado con funciones institucionales o cualquier otro fin personal o ajeno a la administración pública. Su uso indebido podrá ser sujeto de revisión, suspensión de acceso o responsabilidad administrativa conforme a la normatividad aplicable.

Responsabilidad en el respaldo de información institucional

Artículo 31. Será responsabilidad directa del usuario garantizar el respaldo periódico y seguro de la información generada, almacenada o procesada en los equipos de cómputo, dispositivos electrónicos o medios externos bajo su uso o resguardo, siempre que dichos equipos estén destinados al cumplimiento de funciones institucionales.

Dicho respaldo deberá realizarse conforme a los lineamientos y políticas que emita la Dirección, con el propósito de asegurar la integridad, disponibilidad y recuperación de los datos ante cualquier eventualidad, falla técnica o pérdida de información.

La omisión en el cumplimiento de esta obligación podrá afectar la continuidad operativa de los servicios y no eximirá al usuario de la responsabilidad sobre la pérdida o inadecuado manejo de la información oficial.

Actualización del inventario de bienes informáticos

Artículo 32. Los titulares de las dependencias y unidades administrativas que integran la Administración Pública deberán notificar de manera oportuna y documentada a la Dirección de Control Patrimonial cualquier alta, baja, reubicación o modificación en el estado de los bienes informáticos asignados a su área, así como los cambios de los servidores públicos responsables de su resguardo.

Esta notificación será requisito indispensable para mantener actualizados los registros del inventario institucional, garantizar la trazabilidad y control de los activos tecnológicos, y dar cumplimiento a las disposiciones legales y

administrativas en materia de patrimonio municipal y gestión de bienes muebles.

CAPÍTULO SEXTO
MEDIDAS DE PREVENCIÓN EN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Implementación de medidas de prevención para la protección de infraestructura tecnológica

Artículo 33. El Municipio, a través de la Dirección deberá establecer e implementar medidas preventivas que mitiguen los riesgos asociados a contingencias técnicas, ambientales o de seguridad que pudieran afectar la operación de los sistemas institucionales y.la infraestructura tecnológica crítica.

Entre las acciones mínimas a implementar, se considerarán las siguientes:

I. El Centro Principal de Comunicaciones del Municipio deberá estar equipado, al menos, con sistemas de detección de humo y fuego, extintores operativos, controles de acceso físico, suministro eléctrico regulado y climatización mediante aire acondicionado especializado;

II. Deberá implementarse un sistema de seguridad perimetral, como una barrera de control, que filtre y controle el tráfico de información entrante y saliente en las redes de datos del Municipio, a fin de prevenir accesos no autorizados, ciberataques o pérdida de información;

III. Cada uno de los servidores críticos y operativos en ambientes de producción deberá contar con sistemas de energía ininterrumpida, que aseguren la continuidad de servicio ante fallas eléctricas parciales o transitorias; y,

IV. Preferentemente, el Centro Principal de Comunicaciones deberá disponer de plantas de energía eléctrica de respaldo que permitan mantener operativos los servicios esenciales en caso de interrupciones no programadas en el suministro eléctrico.

Estas medidas deberán documentarse y revisarse periódicamente como parte del Plan de Continuidad Operativa y Seguridad Informática del Municipio, conforme a estándares técnicos y mejores prácticas en la materia.

Elementos obligatorios del soporte documental para recuperación de sistemas de información

Artículo 34. Todo sistema de información que se pretenda poner en operación o entrar en ambiente de producción dentro del Municipio, deberá contar, como medida preventiva y requisito previo, con su respectivo soporte documental de

recuperación y operación, el cual será resguardado, actualizado y controlado por la Dirección.

Este soporte documental deberá contener, preferentemente, los siguientes elementos mínimos:

I. Especificaciones técnicas y requerimientos para su instalación;

II. Sistema operativo y versiones compatibles;

III. Estructura y motor de bases de datos utilizadas;

IV. Licencias de software necesarias para su operación legal;

V. Requerimientos mínimos de hardware para ambientes de prueba y producción;

VI. Credenciales de acceso técnico, que incluye usuarios y contraseñas, en caso de ser indispensables, debidamente protegidas conforme a protocolos de seguridad de la información;

VII. Estrategia y cronograma de respaldos de información; y,

VIII. Procedimientos detallados de recuperación ante desastres o fallos críticos.

La inexistencia o entrega incompleta de este soporte documental podrá constituir causa de improcedencia para la puesta en operación del sistema, sin perjuicio de las responsabilidades contractuales o administrativas correspondientes.

Respaldos de sistemas y bases de datos

Artículo 35. Con el fin de garantizar la integridad, disponibilidad y recuperación de la información institucional ante eventuales riesgos, fallas técnicas o contingencias, la Dirección será responsable de ejecutar respaldos diarios de los sistemas y bases de datos que se encuentren bajo su administración.

Dichos respaldos deberán almacenarse en medios seguros, cifrados y protegidos, y deberán estar debidamente identificados con la fecha y hora exacta de su generación, permitiendo su trazabilidad, control y recuperación efectiva.

La Dirección deberá establecer procedimientos documentados para la verificación periódica de la integridad de los respaldos y su restauración, así como mantener políticas internas que regulen su frecuencia, conservación, custodia y eliminación segura, conforme a los lineamientos aplicables en materia de seguridad de la información y continuidad operativa.

Integración de la matriz institucional de respaldos

Artículo 36. La Dirección deberá elaborar y mantener actualizada una Matriz Institucional de Respaldos, en la que se registren de forma sistemática y verificable los sistemas de información propiedad del Municipio que se encuentren bajo su administración.

Dicha matriz tendrá como finalidad asegurar el control, trazabilidad y cumplimiento de las políticas de respaldo y recuperación de información, e incluirá, al menos, los siguientes elementos por cada sistema:

I. Nombre y descripción del sistema respaldado;

II. Política de retención aplicable, incluyendo la periodicidad del respaldo y el tiempo de conservación de las copias;

III. Tipo de respaldo realizado, siendo completo, incremental, diferencial, entre otros; y,

IV. Fecha y hora de ejecución del respaldo.

La matriz deberá estar disponible para fines de auditoría, supervisión técnica y verificación interna, y se actualizará conforme a las modificaciones en la infraestructura tecnológica o políticas institucionales de respaldo y recuperación de desastres.

Actuación en caso de contingencia tecnológica

Artículo 37. En caso de presentarse una contingencia que comprometa la operación, disponibilidad o integridad de los sistemas de información, bienes informáticos, tecnológicos• o de comunicaciones del Municipio, la Dirección deberá notificar de forma inmediata a la Oficialía Mayor, y coordinarse con las Direcciones de Control Patrimonial y, en su caso, con la Dirección de Recursos Materiales, a efecto de implementar las medidas correspondientes.

La Dirección activará las acciones previstas en el Plan Institucional de Recuperación ante Desastres Tecnológicos, conforme al procedimiento vigente, priorizando la protección de la información, la restauración de los servicios críticos y la mitigación de daños operativos.

Asimismo, la Dirección deberá contactar a los prestadores de servicios involucrados con el fin de gestionar, conforme a derecho, la aplicación de garantías, pólizas de seguro o cláusulas contractuales de mantenimiento vigentes, a fin de asegurar la reparación, reposición o continuidad de los bienes afectados.

Responsabilidad de los usuarios en contingencias imputables

Artículo 38. Cuando se determine que una contingencia tecnológica, afectación a sistemas de información o daño a bienes informáticos del Municipio ha sido originada por acciones u omisiones atribuibles a uno o más usuarios, se deberá

proceder al deslinde de responsabilidades conforme a lo establecido en la normativa administrativa y legal aplicable.

La Dirección elaborará el informe técnico correspondiente y lo turnará a la Oficialía Mayor, y en su caso, a la Contraloría Municipal, a efecto de que se determine la existencia de daño patrimonial, perjuicio institucional o violación a disposiciones administrativas, y se actúe conforme al régimen de responsabilidades de los servidores públicos.

Lo anterior, sin perjuicio de las acciones legales, disciplinarias o resarcitorias que resulten procedentes.

CAPÍTULO SÉPTIMO
RESPONSABILIDADES DE LA DIRECCIÓN

Atribuciones y responsabilidades de la Dirección

Artículo 39. La Dirección será responsable de la planeación, administración, operación y supervisión de los recursos tecnológicos institucionales, y tendrá a su cargo las siguientes funciones:

I. Garantizar el suministro y correcto funcionamiento de los serv1c1os de tecnologías de la información y comunicaciones en todas las áreas de la Administración Pública;

II. Administrar los accesos, perfiles y privilegios de los usuarios a los sistemas institucionales, conforme a las solicitudes y autorizaciones emitidas por los titulares de las dependencias respectivas;

III. Gestionar de forma centralizada las licencias de software institucional, incluyendo correo electrónico, antivirus, sistemas operativos y demás aplicaciones autorizadas;

IV. Realizar diagnósticos técnicos de los equipos de cómputo bajo resguardo de las dependencias de la Administración Pública, previa solicitud formal, para efectos de mantenimiento, reparación o baja;

V. Administrar, mantener y brindar soporte técnico a las bases de datos y sistemas de información que se encuentren en operación y producción;

VI. Documentar los procesos de actualización, incidencias técnicas, mejoras y control de cambios en los sistemas desarrollados, asegurando la trazabilidad y soporte documental correspondiente;

VII. Proporcionar asesoría técnica a los usuarios, exclusivamente a través de los canales oficiales definidos, como la mesa de servicio o sistema de tickets de atención;

VIII. Implementar y supervisar las medidas de seguridad informática y de

protección de la información en los sistemas institucionales, conforme a las políticas de seguridad vigentes;

IX. Realizar respaldos periódicos y técnicos conforme a las necesidades de cada sistema, garantizando la integridad y disponibilidad de la información crítica del Municipio; y,

X. Emitir de forma periódica y con la frecuencia que determine la normativa interna, informes de desempeño, cumplimiento técnico, incidencias relevantes y metas operativas alcanzadas, mismos que serán remitidos a la Oficialía Mayor y, en su caso, a las instancias de control correspondientes.

Resguardo institucional de claves y contraseñas de administración

Artículo 40. Las claves, contraseñas y credenciales de administración de los equipos, sistemas, servidores, dispositivos de red y plataformas de comunicaciones que conforman la infraestructura tecnológica del Municipio, deberán ser generadas, administradas y resguardadas exclusivamente por la Dirección.

El acceso a dichas credenciales estará estrictamente limitado al personal técnico autorizado, y su custodia deberá observar los principios de confidencialidad, integridad y trazabilidad, conforme a los protocolos de seguridad establecidos por la Dirección.

La manipulación, divulgación o uso no autorizado de estas claves será considerada una falta grave y dará lugar a las responsabilidades administrativas, civiles o penales que correspondan conforme a la normativa aplicable.

Implementación de acciones de filtrado de contenido en la red institucional

Artículo 41. La Dirección deberá establecer e implementar las medidas técnicas necesarias para el filtrado, restricción o bloqueo de contenido en la red institucional, con el objetivo de prevenir el acceso no autorizado o indebido a sitios o servicios que no guarden relación con las funciones administrativas y operativas del personal del Municipio.

Dichas medidas deberán contemplar, al menos, la prohibición de acceso a plataformas de juegos, entretenimiento, subastas en línea, contenido pornográfico o de carácter sexual explícito, así como cualquier otro tipo de sitio o categoría que sea expresamente determinada por los titulares de las dependencias de la Administración Pública, en atención a las funciones y atribuciones de los colaboradores bajo su cargo.

La Dirección deberá documentar y revisar periódicamente estas políticas de filtrado, asegurando su eficacia, proporcionalidad y compatibilidad con los fines institucionales.

Responsabilidades de la Dirección en materia de telefonía fija Institucional

Artículo 42. La Dirección será responsable de la gestión, operación y supervisión de los servicios de telefonía fija del Municipio, y deberá ejercer las siguientes atribuciones:

I. Evaluar periódicamente el desempeño, cobertura y eficiencia de los servicios de telefonía fija institucional, y en su caso, proponer a la Oficialía Mayor la actualización, reconfiguración o sustitución de dichos servicios, conforme a los requerimientos técnicos y operativos;

II. Emitir dictámenes técnicos sobre las solicitudes de ampliación, instalación de nuevas líneas telefónicas, asignación de equipos o habilitación de extensiones, con base en criterios de funcionalidad, disponibilidad presupuestal y racionalidad administrativa;

III. Administrar, configurar y supervisar el funcionamiento del conmutador telefónico institucional, verificando que los servicios contratados sean prestados conforme a los términos pactados y con calidad adecuada;

IV. Llevar el control y registro actualizado del número de líneas y extensiones telefónicas asignadas a los servidores públicos, así como coordinar con la Dirección de Recursos Humanos la integración y mantenimiento del directorio oficial de números y extensiones; y,

V. Revisar, validar y certificar las facturas correspondientes a los servicios de telefonía fija institucional, para su remisión oportuna a la Dirección de Recursos Materiales a efecto de proceder con su trámite de pago conforme a la normatividad aplicable.

Definición de estándares tecnológicos para sistemas institucionales

Artículo 43. Será responsabilidad exclusiva de la Dirección determinar, establecer y documentar los estándares tecnológicos aplicables al desarrollo, operación y mantenimiento de los sistemas institucionales del Municipio.

Dichos estándares incluirán, de manera enunciativa y no limitativa, la selección y uso de motores de bases de datos, lenguajes de programación, entornos de desarrollo, herramientas tecnológicas, frameworks, protocolos de integración, y cualquier otro componente técnico necesario para garantizar la interoperabilidad, eficiencia, seguridad, escalabilidad y sostenibilidad de los sistemas.

Toda solución tecnológica desarrollada o adquirida por las dependencias de la Administración Pública deberá alinearse a estos lineamientos, salvo justificación técnica debidamente aprobada por la Dirección.

Administración de la red de datos e infraestructura tecnológica

Artículo 44. La Dirección será la instancia responsable de la gestión, operación, monitoreo, mantenimiento, expansión y seguridad de la red de datos institucional y de toda la infraestructura tecnológica del Municipio.

Esta responsabilidad comprende las dependencias de la Administración Pública de los servidores, cableado estructurado, conmutadores, puntos de acceso, equipos de comunicación, centros de datos, nodos de red, así como cualquier componente físico o lógico que forme parte de la arquitectura tecnológica municipal.

La Dirección deberá garantizar la disponibilidad, escalabilidad, integridad y seguridad de dicha infraestructura, conforme a las mejores prácticas en gobernanza de tecnologías de la información, estándares técnicos vigentes y normativa aplicable en materia de ciberseguridad y administración pública digital.

Acciones preventivas y reactivas contra delitos cibernéticos

Artículo 45. La Dirección estará facultada para realizar estudios técnicos, diagnósticos de seguridad, pruebas de vulnerabilidad y análisis de riesgos orientados a identificar posibles amenazas, brechas de seguridad o intromisiones no autorizadas en los sistemas de información, redes, plataformas y servicios digitales del Municipio.

Asimismo, deberá implementar medidas proactivas y reactivas para la prevención, contención y mitigación de delitos cibernéticos, tales como accesos indebidos, sabotajes informáticos, robo o alteración de datos, ataques de denegación de servicio, o cualquier otra conducta ilícita que comprometa la seguridad, confidencialidad, integridad o disponibilidad de los activos digitales municipales.

En caso de detectarse incidentes de seguridad con posible connotación delictiva, la Dirección deberá informar de forma inmediata a la Oficialía Mayor y, en su caso, a la Contraloría Municipal y autoridades competentes, a efecto de que se determinen las acciones legales y técnicas correspondientes.

CAPÍTULO OCTAVO
PRESTACION Y CONTROL DE LOS SERVICIOS DE INTERNET, INTRANET, CORREO ELECTRÓNICO, SISTEMAS, PORTALES Y PÁGINAS WEB DEL MUNICIPIO

Procedimiento para la solicitud de servicios

electrónicos institucionales

Artículo 46. Para efectos de la habilitación y prestación de servicios electrónicos institucionales, tales como cuentas de correo electrónico, acceso a internet, sistemas de información, plataformas digitales e intranet, los titulares de las dependencias y unidades administrativas que integran la Administración Pública, deberán solicitar a la Dirección, a través de los canales oficiales establecidos, el nivel de acceso y tipo de servicio requerido para cada servidor público bajo su responsabilidad.

Toda solicitud deberá estar debidamente justificada y autorizada por el titular correspondiente, con base en las funciones, atribuciones y necesidades operativas del usuario, y será procesada conforme a los protocolos técnicos, de seguridad y control establecidos por la Dirección.

La asignación de dichos servicios estará sujeta a disponibilidad técnica, criterios de racionalidad administrativa y cumplimiento de las disposiciones aplicables en materia de uso responsable de tecnologías institucionales.

Instalación de software y gestión de contenidos en la intranet institucional

Artículo 47. La Dirección será la instancia responsable de atender, evaluar, autorizar e instalar el software necesario en los equipos de cómputo asignados a los servidores públicos, conforme a las solicitudes debidamente justificadas por las dependencias o unidades administrativas, y con base en criterios de compatibilidad, licenciamiento, seguridad y funcionalidad institucional.

Asimismo, los titulares de las dependencias y unidades administrativas que requieran generar, modificar o publicar información en la intranet institucional, deberán designar por escrito, ante la Oficialía Mayor, a un enlace operativo responsable de coordinar con la Dirección las actividades relacionadas con el procesamiento, validación y publicación de dichos contenidos.

La Dirección validará técnicamente el formato, estructura y cumplimiento de las políticas institucionales de contenido, asegurando su integración armónica en los sistemas internos de información.

Acceso controlado y resguardo de instalaciones tecnológicas

Artículo 48. El acceso a las instalaciones físicas donde se ubiquen equipos de cómputo, servidores, dispositivos de administración, distribución o almacenamiento relacionados con los serv1c1os electrónicos y de comunicaciones del Municipio, estará estrictamente restringido al personal técnico autorizado por la Dirección.

Cualquier intento de ingreso no autorizado, modificación, sabotaje, alteración o sustracción de equipos, datos o componentes tecnológicos deberá ser reportado de forma inmediata por la Dirección a la Contraloría Municipal, a efecto de que se proceda al deslinde de responsabilidades y, en su caso, se interpongan las

acciones administrativas, civiles o penales que resulten procedentes conforme a la normatividad vigente.

La Dirección deberá implementar controles de acceso físico y mecanismos de monitoreo adecuados para la protección de dichas instalaciones, conforme a estándares de seguridad y mejores prácticas en infraestructura crítica de tecnologías de la información.

Registro y control de cuentas de correo electrónico institucional

Artículo 49. La Dirección será responsable de la asignación, administración y control de las cuentas de correo electrónico institucional otorgadas a los servidores públicos del Municipio.

Para tal efecto, deberá llevar un registro actualizado que contenga, al menos, el nombre del usuario, unidad administrativa de adscripción, fecha de asignación, nivel de acceso y estatus de la cuenta. Este registro tendrá como finalidad garantizar la trazabilidad, uso adecuado y seguridad de las comunicaciones oficiales.

La Dirección establecerá mecanismos de monitoreo, suspensión o cancelación de las cuentas inactivas o aquellas cuyo uso contravenga las disposiciones normativas o políticas institucionales de uso de servicios electrónicos.

Mecanismos de seguridad para el acceso a cuentas de usuarios

Artículo 50. Con el objeto de proteger la integridad y confidencialidad de las cuentas de usuario que otorgan acceso a los servicios electrónicos institucionales, la Dirección implementará mecanismos automáticos de seguridad que incluyan el bloqueo temporal de la cuenta después de cinco intentos consecutivos fallidos de acceso.

Una vez activado el bloqueo, el usuario deberá reportar el incidente a la Dirección a través de los canales oficiales establecidos, con el fin de verificar su identidad, confirmar el uso legítimo de la cuenta y proceder a su reactivación conforme a los protocolos de seguridad aplicables.

Este mecanismo forma parte de las medidas preventivas de ciberseguridad adoptadas por el Municipio para mitigar riesgos de accesos no autorizados o actividades maliciosas en el entorno digital institucional.

Portales institucionales como medios oficiales de información

Artículo 51. Los portales electrónicos, páginas web oficiales y demás plataformas digitales administradas por el Municipio, constituyen medios legítimos de difusión, divulgación y consulta de información oficial, institucional y de interés público.

La información publicada en dichos medios deberá observar los principios de

veracidad, transparencia, accesibilidad, oportunidad y legalidad, conforme a las disposiciones aplicables en materia de comunicación gubernamental, tecnologías de la información y acceso a la información pública.

La Dirección será responsable de garantizar la integridad, actualización y seguridad del contenido publicado, en coordinación con las dependencias generadoras de la información.

Actualización y gestión de portales y páginas web institucionales

Artículo 52. La Dirección en coordinación con la Dirección General de Comunicación Social, podrá diseñar, desarrollar y actualizar los portales y páginas web oficiales del Municipio, a solicitud expresa y por escrito de los titulares de las dependencias y unidades administrativas de la Administración Pública.

En los casos en que las propias dependencias y unidades administrativas participen directamente en la actualización o generación de contenido para dichos portales, deberán designar formalmente, ante la Oficialía Mayor, a un enlace responsable de coordinar los trabajos técnicos, editoriales y de validación con la Dirección y la Dirección General de Comunicación Social.

El servidor público designado como enlace será responsable del contenido generado, validado y publicado, así como de garantizar que la información difundida cumpla con los principios de veracidad, actualidad, institucionalidad y legalidad, conforme a la normativa aplicable en materia de comunicación gubernamental, transparencia y tecnologías de la información.

Lineamientos para el desarrollo y publicación de portales y páginas web institucionales

Artículo 53. En el diseño, desarrollo, actualización y publicación de portales y páginas web oficiales del Municipio, deberán observarse los siguientes lineamientos normativos y técnicos, con el propósito de asegurar el cumplimiento de estándares legales, éticos e institucionales siguientes:

I. Garantizar el respeto irrestricto a los derechos de autor, propiedad intelectual y privacidad de las personas, evitando la publicación de datos personales, sensibles o de identificación sin el consentimiento correspondiente o fundamento legal;

II. Incorporar en el contenido publicado referencias explícitas al Municipio, presentando de manera clara y coherente el tema, materia o asunto institucional que se pretende difundir;

III. Informar de manera visible y accesible a los usuarios sobre la fuente, vigencia y caducidad de la información publicada, absteniéndose de divulgar datos cuya veracidad, confiabilidad o procedencia no puedan ser comprobadas; y,

IV. Abstenerse de incluir imágenes, gráficos, textos u otros elementos visuales con fines comerciales, publicitarios o de lucro, salvo aquellos de carácter institucional expresamente autorizados.

Las imágenes, tipografías, botones de navegación y demás elementos visuales o funcionales deberán ajustarse a los lineamientos de imagen institucional y contar con la aprobación previa de la Dirección General de Comunicación Social, quien fungirá como autoridad en materia de identidad gráfica y comunicacional del Municipio.

CAPÍTULO NOVENO
GARANTIAS DE LOS BIENES INFORMATICOS Y TECNOLÓGICOS

Garantía de equipos y bienes informáticos

Artículo 54. Todos los equipos, componentes y bienes informáticos que sean adquiridos por el Municipio deberán contar, preferentemente, con garantía técnica en sitio con una vigencia mínima de tres años naturales a partir de la fecha de entrega y recepción formal del bien.

Dicha garantía deberá cubrir defectos de fabricación, funcionamiento, vicios ocultos y fallas técnicas, así como incluir el soporte necesario para su reparación o sustitución sin costo adicional para el Municipio, conforme a las condiciones establecidas en los contratos, órdenes de compra y disposiciones normativas en materia de adquisiciones y bienes muebles.

La Dirección será responsable de verificar el cumplimiento de esta disposición durante el proceso de contratación y recepción de los bienes, así como de dar seguimiento al cumplimiento de la garantía durante su vigencia.

Notificación obligatoria ante daño o desperfecto de bienes informáticos o tecnológicos

Artículo 55. Todo servidor público que tenga bajo su uso o resguardo bienes informáticos o tecnológicos del Municipio tendrá la obligación de notificar de manera inmediata, por escrito o a través de los medios oficiales establecidos, cualquier daño, desperfecto, falla o irregularidad detectada en dichos bienes.

La notificación deberá dirigirse tanto a la Dirección de Recursos Materiales como a la Dirección de Control Patrimonial, con el objeto de que se realicen las gestiones necesarias para determinar el origen del daño, verificar la vigencia de la garantía correspondiente y, en su caso, tramitar la reparación, reposición o procedimiento administrativo aplicable.

Asignación temporal de equipos en calidad de préstamo

Artículo 56. Cuando, por motivo de reparación, sustitución o validación de garantía, un equipo informático o tecnológico deba ser retirado de su lugar de uso, y siempre que las condiciones de disponibilidad lo permitan, la Dirección podrá

asignar al servidor público afectado un equipo en calidad de préstamo temporal.

Esta asignación se realizará exclusivamente con el fin de garantizar la continuidad en el desempeño de sus funciones y estará sujeta a un resguardo formal, especificando el tipo de equipo, condiciones de uso y plazo estimado de devolución.

Una vez concluido el trámite de garantía o reparación, el usuario deberá devolver el equipo prestado en las condiciones en que fue entregado, salvo el deterioro natural por uso razonable.

CAPÍTULO DÉCIMO
DEL USO EN EVENTOS DE LOS BIENES INFORMÁTICOS Y TECNOLÓGICOS

Solicitud de bienes y servicios informáticos para apoyo en eventos o comisiones oficiales

Artículo 57. Las dependencias y unidades administrativas que integran la Administración Pública, así como el personal debidamente autorizado, podrán solicitar apoyo de bienes informáticos, servicios logísticos o soporte técnico por parte de la Dirección para su utilización en eventos institucionales, actos oficiales o comisiones específicas.

La solicitud deberá ser formulada por el titular de la dependencia correspondiente y remitida con la debida anticipación a la Dirección, especificando de forma detallada el lugar, fecha, hora, duración estimada del evento, así como los requerimientos técnicos necesarios.

La Dirección evaluará la viabilidad técnica y disponibilidad del recurso solicitado, a fin de garantizar el cumplimiento eficiente de las actividades institucionales y el uso racional de los bienes tecnológicos.

Instalación de equipo de cómputo para eventos o comisiones oficiales

Artículo 58. La instalación, configuración y puesta en operación de equipos de cómputo, periféricos y demás recursos tecnológicos requeridos para eventos institucionales o comisiones oficiales deberá realizarse exclusivamente por personal técnico autorizado de la Dirección.

Dicha instalación deberá efectuarse en el sitio designado para la realización del evento, en la fecha y hora programadas, garantizando el correcto funcionamiento del equipo y la integridad de la infraestructura tecnológica utilizada.

El personal de la Dirección será responsable de verificar las condiciones de seguridad, conectividad y operación antes, durante y, en su caso, después del evento, conforme a los protocolos establecidos.

Uso institucional del equipo de cómputo asignado para eventos o comisiones

Artículo 59. El equipo de cómputo que sea proporcionado en calidad de préstamo para el desarrollo de eventos, actividades oficiales o comisiones institucionales deberá utilizarse exclusivamente para fines relacionados con las funciones públicas encomendadas y en el marco de las actividades previamente autorizadas.

Una vez concluido el evento o comisión, el equipo asignado deberá ser devuelto a la Dirección en las condiciones en que fue entregado, salvo el desgaste natural derivado del uso adecuado.

La Dirección podrá requerir la firma del acta de entrega-recepción correspondiente, y realizará la verificación técnica del estado del equipo para efectos de control patrimonial y continuidad operativa.

Interpretación y resolución de controversias **Artículo 60.** Los casos no previstos en las presentes Disposiciones Administrativas, así como cualquier controversia, duda interpretativa o conflicto que se derive de su aplicación, corresponderá ser analizada y resuelta por la Dirección en el ámbito de sus atribuciones y conforme al marco normativo aplicable.

En caso de que la naturaleza del conflicto implique la participación de otras unidades administrativas o afecte materias de carácter patrimonial, presupuestal o disciplinario, la Dirección deberá coordinarse con la Oficialía Mayor, la Dirección General Jurídica y, en su caso, con la Contraloría Municipal, para la emisión de un pronunciamiento conjunto o la remisión a la autoridad competente.

ARTÍCULOS TRANSITORIOS

Vigencia

PRIMERO. Las presentes Disposiciones Administrativas entrarán en vigor al día siguiente de su publicación en el Periódico Oficial de Gobierno del Estado de Guanajuato.

Instrumentos normativos

SEGUNDO. En un término no mayor a noventa días naturales contados a partir de la entrada en vigor de las presentes Disposiciones Administrativas, la Dirección en coordinación con de las dependencias de la Administración Pública se elaborarán los instrumentos normativos siguientes:

I. Manuales de usuarios en los diversos temas de las presentes Disposiciones Administrativas;

II. Lineamientos específicos para la gestión, control y monitoreo del uso de los equipos;

III. Plan de Continuidad Operativa y Seguridad Informática del Municipio;

IV. Matriz Institucional de Respaldos;

V. Plan Institucional de Recuperación ante Desastres Tecnológicos; y,

VI. Lineamientos para el desarrollo y publicación de portales y páginas web institucionales.

Se extiende la presente certificación, a los diecisiete días del mes de abril de dos mil veintiséis, para los fines legales correspondientes.

Atentamente

SALAMANCA
SECRETARÍA DEL H. AYUNTAMIENTO

Licenciado Gonzalo Esaú Cano Calvete
Secretario del H. Ayuntamiento