**HONORABLE AYUNTAMIENTO DEL MUNICIPIO DE ATLIXCO ADMINISTRACIÓN 2014-2018**

**REGLAMENTO DE LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y PADRONES**





**H. AYUNTAMIENTO CONSTITUCIONAL ATLIXCO, PUE.**

**2014-2018**

|  |
| --- |
| **FECHA** |
| **11 / Nov/ 2014 ACUERDO de Cabildo con Fecha 11 de Noviembre de 2014 del Honorable Ayuntamiento del Municipio de Atlixco, que aprueba el Reglamento de la Dirección de Tecnologías de Información y Padrones del H. Ayuntamiento de Atlixco.** |

# REGLAMENTO DE LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y PADRONES DEL HONORABLE AYUNTAMIENTO DE ATLIXCO, PUEBLA

**CONTENIDO CAPÍTULO PRIMERO**

DISPOSICIONES GENERALES ARTÍCULOS 1-5

# CAPÍTULO SEGUNDO

DE LA DIRECCIÓN DE TECNOLOGIAS DE ARTÍCULOS 6-7 INFORMACIÓN Y PADRONES

# SECCIÓN PRIMERA

DELA JEFATURA DE DESARROLLO WEB, ARTÍCULOS 8-9 BASE DE DATOS Y PADRONES

# SECCIÓN SEGUNDA

DELA JEFATURA DE REDES Y SOPORTE TÉCNICO ARTÍCULO 10

# SECCIÓN TERCERA

DE LAS FUNCIONES DE INGENIERIA DE PROCESOS ARTÍCULO 11

# CAPÍTULO TERCERO

DE LA RESPONSABILIDAD DE LOS USUARIOS ARTÍCULO 12

# SECCIÓN PRIMERA

DEL USO DEL INTERNET ARTÍCULO 13

# SECCIÓN SEGUNDA

DEL CORREO ELECTRÓNICO INSTITUCIONAL ARTÍCULOS 14-19

# CAPÍTULO CUARTO

DE LA SEGURIDAD DE LA INFORMACIÓN E ARTÍCULOS 20-25 INFRAESTRUCTURA INFORMÁTICA

# CAPÍTULO QUINTO

SANCIONES ARTÍCULOS 26-28

# TRANSITORIOS

**CAPÍTULO PRIMERO DISPOSICIONES GENERALES**

**Artículo 1.-** El presente Reglamento es de observancia obligatoria para toda persona que se desempeñe como empleado, prestador de servicios, practicante, personal administrativo y de confianza del H. Ayuntamiento de Atlixco, dentro de las instalaciones que lo conforman, y que cuenten con equipo de cómputo como herramienta de trabajo así como a invitados que pidan acceso a la red del H. Ayuntamiento de Atlixco.

**Artículo 2.-** Para la observancia y aplicación del presente Reglamento, se entiende por:

**Activo de TIC:** La información, base de datos, programa de computo, un bien informático físico, solución tecnológica, sistema o aplicativo, relacionados con el tratamiento de la misma, que tengan valor para la Institución.

**Autenticación:** El proceso que tiene por objetivo asegurar la identificación de un usuario.

**Confidencialidad:** La característica o propiedad mediante la cual la información está disponible o es revelada a individuos o procesos autorizados.

**Cuenta de correo electrónico:** El identificador único y personal compuesto por el nombre del servidor público de la Institución y una contraseña con el propósito de acceder a recursos o servicios de TIC.

**Datos personales:** La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que este referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad.

**Disponibilidad:** La característica o propiedad de la información, de permanecer accesible para su uso cuando lo requieran individuos o procesos autorizados.

**DTIP:** Dirección de Tecnologías de Información y Padrones.

**Equipo de cómputo:** el conjunto de CPU con todos sus componentes de software y hardware, así como internos, tarjetas de expansión o componentes externos como bocinas o módems sin ser estos los únicos existentes, monitor, teclado y ratón.

**Equipo de impresión:** A todas las impresoras de cualquier modelo, tipo o marca que sirva como interfaz de salida física en papel u otro medio de las computadoras.

**Estrategia:** Las líneas de acción definidas para establecer en el ámbito de la Administración Municipal, la política de gobierno digital orientada al ordenamiento de TIC, la cual está sustentada en un marco rector de procesos diseñado con base en las mejores prácticas nacionales e internacionales en materia de TIC.

**Evento** La alerta o notificación creada por un servicio de TI, elemento de configuración o herramienta de monitorización. Los eventos requieren normalmente que el personal de operaciones de TI tome acciones, y a menudo conllevan al registro de incidentes.

**Firma Electrónica Avanzada:** El conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a que se refiere, lo que permite que sea detectable cualquier modificación, y que produce los mismos efectos que la firma autógrafa.

**Funcionalidad:** Las características de un servicio de TIC que permiten que cubra las necesidades o requerimientos de un usuario.

**Gobierno digital:** Las políticas, acciones y criterios para el uso y aprovechamiento de las tecnologías de información y comunicaciones, con la finalidad de mejorar la entrega de servicios al ciudadano; la interacción del gobierno con la industria; facilitar el acceso del ciudadano a la información de este, así como hacer más eficiente la gestión gubernamental para un mejor gobierno y facilitar la interoperabilidad entre las Instituciones.

**Incidente:** La interrupción no planificada de un servicio de TIC o reducción en la calidad de un servicio de TIC.

**Infraestructura de TIC:** El hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorizar, controlar o soportar los servicios de TIC. El termino infraestructura de TIC incluye todas las TIC pero no las personas, procesos y documentación asociados.

**Integridad:** Mantener la exactitud y corrección de la información y sus métodos de proceso.

**Plan de contingencia:** El documento en el que se plantea la estrategia, los servidores públicos y las actividades requeridas, para recuperar por completo o parcialmente un servicio o proceso crítico, en caso de desastre, derivado de que se presente un riesgo.

**Problemas:** El evento o incidente del cual se plantea una solución alterna, no se tiene conocimiento de su origen y se espera de una solución definitiva.

**PMI**: Por sus siglas en inglés, Project Management Institute, cuyo objetivo principal es la administración de proyectos.

**PUMA:** Padrón Único del Municipio de Atlixco; plataforma tecnológica en bases de datos, unificada, centralizada, normalizada y estandarizada de consulta eficaz de información y generación de reportes. Permite tomar decisiones focalizadas y centradas a resolver problemáticas en tiempo, forma y con la calidad deseada, con un seguimiento estratégico, puntual e inmediato, mediante panel de consultas y reportes. Incluye los módulos de empadronamiento y cobros de mercados y tianguis.

**Recursos de TIC:** La infraestructura, activos, personal especializado, presupuesto y cualquier otro elemento de TIC.

**Repositorio:** El espacio en medio magnético donde se almacena y mantiene la información digital, habitualmente bases de datos o archivos informáticos.

**Riesgo:** La amenaza sobre los activos de TIC, al presentarse puede causar una pérdida o daño sobre estos, puede ser producto de una vulnerabilidad y debe preverse su mitigación.

**Rol:** Los papeles que se desempeñan en la DTIP en los procesos del “Marco rector de procesos en materia de TIC”. A cada papel que se define se le asignan diversas actividades, con independencia de aquellas que por su cargo deba desempeñar el servidor público al que se asigna un determinado rol.

**Seguridad de la información:** La capacidad de preservación de la confidencialidad, integridad y disponibilidad de la información.

**Servicios:** Actividades que desarrollan o coordinan en la DTIP encaminadas a la satisfacción de las necesidades que en materia de TIC requieren las unidades responsables.

**Sistema o aplicativo:** El conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos.

**TIC:** Tecnologías de la Información y la Comunicación, es el conjunto de tecnologías que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de información, en forma de voz, imágenes y datos.

**UML:** por sus siglas en inglés, Unified Modeling Language, es el lenguaje de modelado de sistemas de software, lenguaje gráfico para visualizar, especificar, construir y documentar un sistema.

**Unidad responsable:** Las unidades administrativas de la Institución que para el desarrollo de sus funciones requieren de los servicios que proporciona la UTIC.

**Usuarios:** Los servidores públicos que en el desempeño de sus funciones hacen uso de los servicios de TIC.

**Verificación:** La actividad que permite revisar si un servicio de TIC, plan, proceso o cualquier otro producto o entregable, está completo y acorde con su especificación de diseño.

**Vulnerabilidad:** La debilidad en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a un activo de TIC.

**Artículo 3.-** Los equipos de cómputo son única y exclusivamente equipo de apoyo para desempeñar las funciones propias de las dependencias del Ayuntamiento.

**Artículo 4.-** Las partes y dispositivos que conforman la computadora, como las unidades lectoras, memorias RAM, discos duros, monitores, son propiedad del Municipio y éstos no podrá ser extraído o removido sin previa autorización de la DTIP.

Los equipos de cómputo serán removidos y/o dados de baja, mediante dictamen emitido por el Titular de la DTIP.

# Artículo 5.- De la propiedad de la Información.

La información propiedad del municipio, es la siguiente:

1. La que sea grabada o respaldada en los medios de almacenamiento de los equipos de cómputo propio o ajenos, producto de las labores diarias;
2. La que se genere por los usuarios de Tecnologías de la Información;

La información considerada como propiedad municipal no podrá ser extraída para su uso fuera de las instalaciones, por ningún medio de almacenamiento; de igual manera aplica para medios de comunicación como son Internet, unidades de comunicación inalámbrica o portátil como teléfonos celulares o computadoras. En caso de ser necesaria la sustracción se deberá de especificar el tipo de información y el motivo para el que será destinado, solicitando la autorización correspondiente al Titular de la DTIP.

# CAPÍTULO SEGUNDO

**DE LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y PADRONES**

**Artículo 6.-** Son facultades y atribuciones de la Dirección de Tecnologías de Información y Padrones:

1. Proponer al Presidente y al H. Cabildo la “Estrategia General de Tecnologías de Información y Comunicaciones” para el municipio de Atlixco dentro del Plan Municipal de Desarrollo, así como las normas y lineamientos para regular el desarrollo informático y de telecomunicaciones y vigilar la aplicación de los mismos, así como proponer al Presidente los proyectos tecnológicos que apoyen los procedimientos administrativos, operativos y de servicios de las áreas internas y organismos del Ayuntamiento;
2. Coordinar y dirigir el desarrollo, implementación y administración de proyectos de tecnologías de información y comunicaciones para el análisis, diseño, desarrollo y mantenimiento de sistemas de información, bases de datos, Padrón Único Municipal y/o aplicaciones, con el fin de contribuir a la sistematización y mejora continua de los procesos operativos del Ayuntamiento;
3. Establecer las estrategias y metodologías para la construcción de bases de datos operacionales, estadísticas, analíticas y geográficas del Ayuntamiento, con el propósito de garantizar que el uso y consulta de la información contenida en dichas bases de datos, cumpla con los atributos de seguridad, calidad, oportunidad y veracidad;
4. Establecer y vigilar el cumplimiento de las políticas, normas, estándares y lineamientos en materia de tecnologías de comunicaciones e información, así como definir y coordinar los procesos necesarios para su cumplimiento y asegurar su difusión;
5. Coordinar e impulsar los planes de verificación, consolidación e integración de la información en las bases de datos del Padrón Único de Beneficiarios que se generan en los diferentes procesos de los Programas Sociales del Ayuntamiento;
6. Establecer y coordinar los planes de servicio, mantenimiento y fortalecimiento de los recursos informáticos y de telecomunicaciones del Ayuntamiento;
7. Asegurar la administración de la infraestructura tecnológica de equipos de telecomunicaciones, bases de datos del “PUMA” y sistemas de información del Ayuntamiento;
8. Dictaminar, verificar, apoyar y supervisar los aspectos técnicos en las adquisiciones de bienes informáticos así como las asesorías, consultorías, en servicios informáticos y de telecomunicaciones en estrecha relación y coordinación con la Dirección de Recursos Materiales y Tesorería del Ayuntamiento;
9. Coordinar y supervisar los mecanismos que aseguren el crecimiento de la cultura de la información mediante procesos de capacitación, difusión, asesoría y apoyo en el conocimiento y uso de la tecnología de información a los diferentes usuarios del Ayuntamiento;
10. Participar y apoyar en los procesos de planeación estratégica en materia de TIC;
11. Definir las políticas, estrategias, lineamientos, normas y procedimientos para la administración del “PUMA”;
12. Coordinar y supervisar las etapas de análisis, diseño, construcción, implantación y mantenimiento de los Sistemas de Información y Telecomunicaciones;
13. Determinar lineamientos seguros y eficientes para la explotación de la información referente al Padrón Único Municipal;
14. Contribuir a que el Ayuntamiento cuente con los indicadores de resultados necesarios, para difundir la operación de los programas así como con información que apoye la mejor toma de decisiones;
15. Coordinar la implementación de mecanismos para el registro y la atención de solicitudes de información estadística;
16. Evaluar y aprobar los nuevos requerimientos de información estadística con el propósito de generar procesos automatizados que faciliten solicitudes subsecuentes;
17. Proponer mecanismos de control y seguimiento operativo sobre los procesos en las áreas del Ayuntamiento que impliquen el mantenimiento de las bases de datos centrales;
18. Autorizar el acceso y uso de los sistemas de la red de área local (LAN interna o extendida), delegando en caso necesario esta facultad al personal del área que corresponda, de acuerdo a las necesidades del servicio;
19. Implementar acciones que permitan garantizar la confidencialidad, seguridad e integridad de la información contenida en las bases de datos centrales;
20. Proponer acciones de coordinación con dependencias federales, estatales y organismos municipales para el desarrollo de proyectos de aplicación tecnológica para el municipio de Atlixco;
21. Las demás que resulten de las disposiciones legales y administrativas aplicables.

**Artículo 7.-** Son facultades del Director de Tecnologías de Información y Padrones:

1. Coordinar la integración de información a las bases de datos centrales de las diferentes áreas del Ayuntamiento en una plataforma tecnológica central que permita la unificación y estandarización de los datos;
2. Normar la construcción de modelos de captura de las bases de datos de los procesos y/o programas a cargo de las unidades administrativas del Ayuntamiento;
3. Diseñar y operar un “sistema único” de actualización de registros de las bases de datos centrales;
4. Diseñar la estrategia operativa que permita proteger la información recolectada dentro de las bases de datos centrales;
5. Establecer y operar los sistemas, así como los procedimientos para la integración y actualización de las bases de datos centrales;
6. Diseñar y desarrollar una plataforma informática que posibilite el análisis multidimensional de la información estadística y espacial para la planeación, diseño y evaluación de la toma de decisiones en política económica social;
7. Coordinar la actualización de las bases de datos de los procesos e indicadores de ingresos, económicos, políticos y sociales;
8. Generar mecanismos técnicos de georreferenciación a nivel municipal, por junta auxiliar y localidad sobre los datos, procesos e indicadores de las diferentes áreas del Ayuntamiento;
9. Proporcionar información estadística y geográfica que requieran las áreas del Ayuntamiento para el desempeño de sus funciones.

# SECCIÓN PRIMERA

**DE LA JEFATURA DE DESARROLLO WEB, BASES DE DATOS Y PADRONES**

**Artículo 8.-** La Jefatura de Desarrollo Web, Bases de Datos y Padrones dependerá directamente de la Dirección de Tecnologías de Información y Padrones y tendrá las atribuciones siguientes:

1. Coordinar y supervisar las etapas de análisis, diseño, construcción, implantación y mantenimiento de los Sistemas de Información, apoyados en metodologías de gestión de proyectos como el PMI y de lenguajes de modelado UML;
2. Supervisar la correcta aplicación de las metodologías y estándares de desarrollo durante el ciclo de vida de los Sistemas de Información;
3. Ejecutar las tareas de administración y respaldos de bases de datos, necesarias para garantizar el óptimo desempeño en el manejo de la información;
4. Administrar los accesos de los usuarios a las bases de datos bajo la definición de autorizaciones y permisos para su uso;
5. Elaborar los controles operativos y técnicos para realizar las actualizaciones a los sistemas de las bases de datos, con el propósito de garantizar la mejora continua;
6. Diseñar las Bases de Datos, Sistemas y aplicaciones, basándose en la metodología de UML, aplicándola al diseño preliminar de pantallas, arquitectura de las bases de datos, selección de hardware y software para su desarrollo y pruebas a sistemas;
7. Dirigir, coordinar, elaborar y supervisar las actividades de definición, planeación e implementación relacionadas a la arquitectura de bases de datos y aplicación de las metodologías PMI y UML;
8. Proponer, diseñar y coordinar los proyectos tecnológicos que soporten la operación de los procesos de las áreas del Ayuntamiento, apoyándose en la metodología PMI;
9. Establecer y coordinar los planes de servicio, mantenimiento y fortalecimiento de los recursos informáticos y de telecomunicaciones;
10. Asegurar la operación y administración de la infraestructura tecnológica de equipos de telecomunicaciones, cómputo y sistemas de información;
11. Coordinar y supervisar la adquisición de bienes y servicios informáticos y de telecomunicaciones en coordinación con el área de recursos financieros y materiales del Ayuntamiento;
12. Las demás que resulten de las disposiciones legales y administrativas aplicables.

**Artículo 9.-** Son funciones de la Jefatura de Desarrollo Web, Bases de Datos y Padrones, en relación al PUMA, las siguientes:

1. Establecer los lineamientos, procesos y mecanismos de análisis de datos que garanticen la integridad y la calidad de la información;
2. Establecer los lineamientos, procesos y mecanismos para la liberación de información ante las áreas operativas y de indicadores del Ayuntamiento;
3. Coordinar y supervisar la aplicación de las actualizaciones para el mantenimiento;
4. Identificar y depurar la funcionalidad de los sistemas relacionados con el manejo y control que permitan mejorar su funcionalidad, mediante requerimientos al área de Desarrollo de Software y Bases de Datos;
5. Coordinar que se documente y genere información de seguimiento de los procesos operativos de su responsabilidad;

# SECCIÓN SEGUNDA

**DE LA JEFATURA DE REDES Y SOPORTE TÉCNICO**

**Artículo 10.-** La Jefatura de Redes y Soporte Técnico dependerá directamente de la Dirección de Tecnologías de Información y Padrones y tendrá las atribuciones siguientes:

* 1. Establecer y dirigir el desarrollo informático y de telecomunicaciones, desarrollar proyectos tecnológicos de infraestructura de redes y comunicaciones, de manera unificada, centralizada y estandarizada;
  2. Establecer y coordinar los planes de servicio, mantenimiento y fortalecimiento de los recursos informáticos y de telecomunicaciones.
  3. Asegurar la administración de la infraestructura tecnológica de equipos de telecomunicaciones, servidores, switching, cómputo y sistemas de información.
  4. Coordinar las actividades de servicio en soporte técnico, implementando tareas ágiles y concisas, administrando al personal de la Jefatura y al de Servicio Social para dar una respuesta pronta a las solicitudes de usuarios que tenga como herramienta de trabajo una computadora o algún otro dispositivo tecnológico, que necesiten resolver determinados problemas como la instalación de hardware o software y asesoría en la utilización de los mismos;
  5. Implementación de redes cableadas e inalámbricas (WIFI) con seguridad informática;
  6. Revisar y diagnosticar hardware que ha sido dado de baja, para posible re- utilización del mismo en dado caso de que sea favorable el diagnostico;
  7. Asegurar la administración, control y monitoreo de manera central y unificada de toda la infraestructura tecnológica patrimonio municipal de redes, swicheo, APs, video-vigilancia interna y municipal. Así como la administración total del “Centro de Datos del Municipio de Atlixco, CEDAMA”, “Centro de Operaciones de Redes del Municipio de Atlixco, CORMA”, “Sistema de Video-vigilancia del Municipio de Atlixco, SIVIVMA”, “Centro de Monitoreo del SIVIVMA” y de la red de área local (LAN interna o extendida)”;
  8. Establecer y administrar el filtrado de contenido y monitoreo para el buen uso de la red municipal e internet institucional;
  9. Administrar, configurar e integrar los servicios tecnológicos de los servidores institucionales de correo, aplicaciones, web, asegurando la seguridad, integridad y disponibilidad de dichos servicios mediante la protección física y lógica con las que se cuente en la DTIP, utilizando y respetando los protocolos de atención y soporte tecnológico que en su caso apliquen;
  10. Realizar seguimiento y verificación a los “soportes y mantenimientos tecnológicos” al Sistema de Video-vigilancia del Municipio de Atlixco, SIVIVMA, mediante los protocolos y formatos de control de atención a dichos soportes. La verificación y atención de los soportes será llevado a

cabo en dos vertientes: 1.- Cuando exista un proveedor externo que otorgue una “póliza de mantenimiento preventivo y correctivo” que cubra la operatividad del SIVIVMA y 2.- Cuando dicha póliza no exista, en cuyo caso la propia DTIP sea la encargada de dar dichos soportes y mantenimientos; En cualquiera de las dos vertientes se aplicaran los controles, protocolos y formatos ya prestablecidos para dar un servicio de mantenimiento al SIVIVMA de manera puntual y eficiente;

* 1. Las demás que resulten de las disposiciones legales y administrativas aplicables.

# SECCIÓN TERCERA

**DE LAS FUNCIONES DE INGENIERÍA DE PROCESOS**

**Artículo 11.-** Son funciones de la DTIP:

* + 1. Planificar, administrar, coordinar y supervisar los trabajos pertenecientes a los diferentes proyectos a cargo del área;
    2. Detecta, evalúa, y propone a través del análisis organizacional y de requerimientos el diseño de nuevos procesos o mejora de los mismos, que coadyuven en la optimización y calidad de los servicios que presta;
    3. Revisa y aprueba los productos documentales necesarios que de acuerdo a la metodología aplicable son generados para que sirvan de instrumento en la modificación o desarrollo de nuevas aplicaciones de software y en el diseño y funcionalidad de las páginas Web Institucionales;
    4. Proponer diferentes formas para ejecutar procesos gubernamentales más eficientes, así como nuevas formas de comunicación dentro y fuera del gobierno;
    5. Planificación de proyectos;
    6. Coordinación de actividades del personal a su cargo; y
    7. Supervisión de todas las actividades técnicas de su área.

# CAPÍTULO TERCERO

**DE LA RESPONSABILIDAD DE LOS USUARIOS**

**Artículo 12.-** Es responsabilidad de los usuarios de los servicios de equipo de telemático, hardware y software las siguientes obligaciones y atribuciones:

1. Los usuarios deben utilizar y respetar el equipo de telemático, hardware y software de acuerdo con el presente reglamento;
2. El Titular de la DTIP, Titulares de las Áreas, Colaboradores de Tecnologías de la Información y Padrones, no podrán utilizar, ni difundir la información personal o confidencial obtenida voluntaria o involuntariamente a través de los procesos de mantenimiento, operación o uso de los servicios y recursos tecnológicos y/o red de datos. Así

mismo, en todo caso queda expresamente prohibido la suplantación de usuario para la realización de cualquier actividad; y

1. Corresponderá en primera instancia al Titular de la DTIP la restricción de acceso de los servicios informáticos a aquellas personas que por sus actuaciones intencionadas perturben seriamente el normal desarrollo de los servicios informáticos y/o tengan actuaciones contrarias a lo establecido en el presente reglamento. Contra dichas actuaciones será de aplicación la Ley de Responsabilidades de los Servidores Públicos del Estado de Puebla.

# SECCIÓN PRIMERA DEL USO DEL INTERNET

**Artículo 13.-** Las autorizaciones de uso de la Internet Institucional a través de la Red Municipal están orientadas a proporcionar a los servidores públicos con acceso a dicha infraestructura, una herramienta de comunicación y apoyo a las actividades que se desarrollan en las Dependencias que conforman la Administración Pública Municipal. En tal sentido, se considera el servicio de Internet Institucional como una herramienta de uso controlado y limitada al trabajo:

1. El área de la DTIP, establecerá de acuerdo a sus funciones y necesidades, la asignación del servicio de Internet a los servidores públicos adscritos a los áreas administrativas. También podrá proporcionar el Servicio de Internet a personal externo que mantenga algún tipo de relación laboral con el Ayuntamiento y que sea necesario para el desempeño de sus actividades, previa solicitud del titular del área apegándose a los lineamientos establecidos para ello;
2. El usuario es responsable directo del uso que dé a su acceso al Internet y por tanto responderá a cualquier irregularidad que se presente en dicho uso como lo es, perdida de sus datos o registros por causas de diseminación de virus u otro tipo de programas que dañen sistemas de proceso de información. Para evitar esto, es obligación del usuario hacer copias y/o respaldos de la información contenida en su computadora, así como depurar periódicamente la información contenida en su buzón de correo institucional;
3. En caso de desconocer las herramientas para la realización de estas acciones, el usuario podrá solicitar asistencia al área de la DTIP;
4. El Administrador del Servicio de Internet, es responsable del análisis, inspección y control de los accesos al internet Institucional con el objeto de que sea utilizado adecuadamente. La solicitud de acceso al servicio de Internet, se realizará de acuerdo al proceso siguiente:
   1. El Titular de la Dependencia, deberá solicitar vía oficio al Titular de la DTIP.
   2. El Titular de la DTIP turnará la solicitud del Servicio de Internet al administrador, quien evaluará su viabilidad y en su caso realizará el alta en el servidor;
5. El Administrador del Servicio de Internet deberá mantener controles que le permita conocer los identificadores tanto del usuario como del equipo de cómputo;
6. El servicio de Internet estará vigente mientras el usuario mantenga su relación laboral con el Gobierno Municipal o hasta que el titular del área solicite la cancelación correspondiente. Es responsabilidad de los titulares de las dependencias municipales, informar a la DTIP los cambios de adscripción o renuncias de los servidores públicos a su cargo, para que ésta proceda a su restricción o baja del servicio que le fue asignado al usuario;
7. El servicio de Internet es provisto por un carrier telefónico y se utilizará exclusivamente como una herramienta de trabajo y la DTIP podrá suspenderlo en los casos que el usuario contravenga la normatividad aplicable o bien cuando se preste mantenimiento a las instalaciones o equipos, falta de corriente eléctrica, tráfico malicioso, virus y spam, o por razones administrativas, entre otras, para lo cual la DTIP, notificará a los usuarios de Internet de la interrupción del servicio cuando se trate de eventos controlados;
8. El usuario se apegará obligatoriamente a los esquemas de operación, seguridad y especificaciones de funcionamiento del Internet.

# SECCIÓN SEGUNDA

**DEL CORREO ELECTRÓNICO INSTITUCIONAL**

**Artículo 14.-** Las cuentas autorizadas de Correo Electrónico Institucional deberán utilizarse exclusivamente para actividades que estén relacionadas con los propósitos y funciones institucionales que desempeñen los servidores públicos, en este sentido, se considera el servicio de Correo Electrónico Institucional como una herramienta de uso controlado y limitado al trabajo.

En el caso de las cuentas de Correo Electrónico Personal, El Titular de las Dependencias, determinará a los servidores públicos que tendrán acceso a estas mediante el servicio de internet y durante la jornada laboral.

La DTIP establecerá de acuerdo a su estructura organizacional y en la medida de lo posible, la asignación de cuentas de Correo Electrónico Institucional a los servidores públicos que el Titular de la Dependencia determine, siendo estos últimos quienes señalen cuál será la contraseña para el acceso a dicha cuenta.

Las cuentas de Correo Electrónico Institucional deberán ser identificadas y registradas, deberán ajustar sus medidas de seguridad en la nomenclatura de las cuentas de usuarios a los siguientes estándares:

1. El nombre de Usuario se puede conformar por 6 caracteres como mínimo y 20 caracteres como máximo, es necesario utilizar únicamente los siguientes caracteres: letras minúsculas “a b c d e f g h i j k l m n o p q r s t u v w x y z”, dígitos “0 1 2 3 4 5 6 7 8 9”, el guion “\_” y el punto “.” solo para casos especiales. No se incluirán acentos, “ñ”, ningún otro carácter especial como espacios en blanco “ / | { } : ; + \* ? ¡ < >;
2. La cuenta se compondrá con el primer nombre, punto y apellido paterno, agregándole dominio correspondiente; Ejemplos validos: [david.martinez@atlixco.gob.mx](mailto:david.martinez@atlixco.gob.mx) ;
3. De haber duplicados o algún caso especial, estos deberán resolverse a criterio del Administrador del Servicio;
4. En el caso de las Dependencias Municipales, será el nombre de la dependencia y la del dominio correspondiente, ejemplo: ingresos@atlixco.gob.mx; y
5. Tratándose de cuentas genéricas se aplicarán las restricciones de los párrafos I, II y III y el nombre deberá de relacionarse con el propósito por que fue creada, ejemplo: [webmaster@atlixco.gob.mx](mailto:webmaster@atlixco.gob.mx)

**ARTÍCULO 15.-** El acceso al servicio de Correo Electrónico Institucional, se realizará de la siguiente forma:

1. El acceso a dicho servicio se realizará mediante el nombre de usuario y contraseña a través de una aplicación Cliente de Correo Electrónico;
2. El Usuario también podrá acceder por Internet a este servicio a través de la Webmail y dirección que para tales efectos determine la DTIP; y
3. El nombre de Usuario y contraseña se deberán de apegar obligatoriamente a los esquemas de operación, seguridad y especificaciones de funcionamiento del Correo Electrónico Institucional propuestos por la DTIP.

**ARTÍCULO 16.-** El manejo de las cuentas, información y contraseñas del servicio de Correo Electrónico Institucional, deberá cumplir con los siguientes requerimientos de seguridad:

1. El nombre de usuario de acceso a la Red Municipal es personal e intransferible, por lo que el uso y el manejo de las mismas, así como la contraseña correspondiente, es responsabilidad absoluta del Usuario;
2. La información trasmitida mediante el servicio de Correo Electrónico Institucional es responsabilidad única y exclusiva del Usuario;
3. El contenido de los mensajes de Correo Electrónico Institucional no goza de validez jurídica, solo hasta que se autorice la utilización de un medio o firma electrónica que le otorgue ese valor jurídico;
4. En virtud de que son los Usuarios quienes crean su propia contraseña, no deberán relacionar la misma con datos personales como son fecha de nacimiento, nombre, apellidos, nombre de sus hijos, sobrenombre, entre otros; y
5. Es responsabilidad del Usuario cambiar cada determinado tiempo su contraseña, de acuerdo al grado de confidencialidad de la información que maneje conforme lo establezca la DTIP.

**ARTÍCULO 17.-** En el caso de que un Usuario olvide su contraseña deberá notificarlo al administrador del servicio para su recuperación. En el supuesto de que un usuario considere que su clave de acceso ha sido divulgada, solicitará su cancelación y la asignación de una nueva. El usuario podrá hacer directamente los cambios de contraseña, cuando las opciones del servicio de web mail lo permitan:

1. El servicio de Correo electrónico Institucional y las contraseñas estarán vigentes mientras el Usuario mantenga una relación laboral con el Gobierno Municipal, o hasta que el Titular Inmediato del Usuario solicite la cancelación correspondiente. Asimismo las Dependencias Municipales tendrán la responsabilidad de notificar a la DTIP, los cambios de adscripción, funciones y renuncias de los servidores públicos, para que esta haga las modificaciones que corresponda o proceda a la baja del servicio dado al Usuario;
2. El servicio de Correo Electrónico Institucional no debe ser utilizado para el almacenamiento de archivos a largo plazo o de acceso esporádico; será herramienta de trabajo diario para facilitar el transporte de los archivos siempre y cuando sea temporal, o de comunicación, evitando el almacenamiento masivo.

**ARTÍCULO 18.-** En ningún caso el usuario hará uso del servicio de Correo Electrónico Institucional un medio para fines personales, políticos, comerciales o publicitarios:

1. Es obligación del Usuario hacer copias y/o respaldos de la información contenida en su buzón, así como depurar periódicamente la información contenida en el mismo, en caso de desconocer las herramientas para la realización de estas acciones, podrá solicitar asistencia a la DTIP;
2. En caso de que un Usuario requiera mayor capacidad de almacenamiento para el Correo Electrónico Institucional, deberá solicitarlo por escrito al Titular de TIGE, quien realizará la evaluación tal requerimiento de acuerdo a las funciones y necesidades del puesto que este desempeñe;
3. El tamaño máximo de los mensajes que pueden ser enviados es de 50 MB, dicha capacidad podrá ser modificada posteriormente por DTIP de acuerdo a las capacidades técnicas de los prestadores del Servicio de Correo Institucional o a las modificaciones que se emiten a los presentes lineamientos;
4. Los mensajes con programas ejecutables serán bloqueados por el Administrador del Servicio con fines de seguridad;
5. La DTIP por conducto del Administrador puede en cualquier momento, suspender una cuenta por inactividad, cuando en un periodo de 90 días naturales no exista acceso al servicio, eliminando el contenido íntegro de

los buzones de correo inactivos o en los casos en que el Usuario contravenga la normatividad aplicable;

1. El servicio de Correo Electrónico Institucional es ininterrumpido. Sin embargo, la DTIP, se reserva el derecho a suspenderlo por causas de fuerza mayor, como el mantenimiento de instalaciones y equipos, desastres naturales, falta de corriente eléctrica, razones administrativas, etc., se notificará a los Usuarios de Correo Electrónico Institucional de la interrupción del servicio cuando se trate de eventos controlados;
2. El Usuario deberá notificar a la DTIP de manera fehaciente e inmediata cualquier uso no autorizado de su cuenta o cualquier otra vulnerabilidad de su integridad, con el objeto de tomar las medidas necesarias y darle solución a la eventualidad.

**ARTÍCULO 19.-** Queda prohibido a los usuarios, la realización de los siguientes actos por medio del correo Electrónico Institucional:

1. Falsificar encabezados de otros mensajes, enviar archivos adjuntos que contengan virus, programas o códigos con capacidad para dañar equipo de cómputo de terceros;
2. Trasmitir mensajes de correo electrónico que infrinjan alguna ley relativa al correo spam o masivo;
3. Hacerse pasar por alguna otra persona, hacer declaraciones falsas, falsificar la identidad de otra persona y realizar actos de difamación;
4. Revisar, copiar, alterar o destruir el contenido del correo electrónico de otro usuario, sin el consentimiento explícito del afectado;
5. Transferir información que afecte los derechos de autor o propiedad intelectual;
6. Intimidar o insultar a otros usuarios o a personas externas a la Dependencia Municipal;
7. Utilizarlo como medio para cualquier propósito político, religioso, bélico, racista, terrorista o cualquier otra que no se relacione a las funciones del servidor público;
8. Obtener o transmitir materiales con contenido obsceno o pornográfico;
9. Realizar actos comerciales, de lucro o publicitarios;
10. Otorgar acceso a terceros y/o coaligarse con infractores cibernéticos; y
11. Cualquier otro análogo a los anteriores.

# CAPÍTULO CUARTO

**DE LA SEGURIDAD DE LA INFORMACIÓN E INFRAESTRUCTURA INFORMÁTICA**

**ARTÍCULO 20.-** La seguridad y el acceso al centro de proceso de datos, servidores o equipo de cómputo que funja como servidor y demás equipos propiedad del Ayuntamiento, será responsabilidad del área de la DTIP y estará a cargo del área de Redes y Soporte Técnico o la que para el efecto se cree.

**ARTÍCULO 21.-** Para los efectos de medidas de seguridad de la información e infraestructura informática, se considerarán los siguientes apartados:

* 1. Medidas de seguridad para equipo informático;
  2. Seguridad en el Servicio de Internet;
  3. Seguridad en los Servidores;
  4. Seguridad en las Aplicaciones y Sistemas;
  5. Seguridad en Aplicaciones sobre servicios Web;
  6. Seguridad sobre la transferencia de Datos;
  7. Servicios de confidencialidad en la Base de Datos; y
  8. Respaldo de los Sistemas y Aplicaciones.

**ARTÍCULO 22.-** Corresponde a la DTIP, implantar las medidas de seguridad para equipo informático y será el personal de esta área el único responsable de instalar el Software básico para uso de computadoras de escritorio o portátiles. En el caso de requerir de la instalación de alguna licencia de Software diferente a la entregada originalmente, deberá de solicitarse a la DTIP con la justificación correspondiente, para que determine su procedencia. En caso de que la licencia deba ser instalada por un tercero, esta deberá estar supervisada por personal autorizado de DTIP:

1. Los equipos no deben tener habilitados los puertos de comunicación (USB, paralelo, serial, etc.), los dispositivos de almacenamiento removible ni los dispositivos de conexión inalámbrica (Wi-Fi, Bluetooth, infrarrojo, etc.), a excepción de los que hayan sido previamente autorizados por el la DTIP;
2. Por el riesgo que implica, está estrictamente prohibido el uso de dispositivos de almacenamiento externo para la trasmisión de información confidencial en soportes electrónicos, mediante traslado físico;
3. El acceso a equipos informáticos con el propósito de realizar labores de mantenimiento preventivo y correctivo o para soporte técnico, es exclusivo para el personal autorizado de la DTIP y/o para un proveedor externo contratado para tal efecto;
4. En caso de información confidencial y/o de uso compartido, el usuario deberá solicitar acceso a los servidores centrales de la Red Municipal para el resguardo de la misma, indicando al personal autorizado de DTIP, los niveles de acceso y usuarios autorizados para agregar, cambiar o eliminar información;
5. En caso de que exista la necesidad extraordinaria de solicitar se habilite algún servicio restringido en los presentes lineamientos, este deberá ser solicitado por escrito o correo electrónico a la DTIP, exponiendo la justificación correspondiente y su autorización dependerá del resultado del análisis;
6. No se permite el tráfico de correo electrónico “SMTP” directo, el tráfico de correo se realizará exclusivamente por medio del servidor central de correo electrónico interno, lo cual evitará que se propaguen virus que intenten mandarse a sí mismos por este medio.

**ARTÍCULO 23.-** Está estrictamente prohibido ejecutar programas encargados de analizar el tráfico de la Red Municipal, sistemas que intenten adivinar las

contraseñas alojadas en las tablas de usuarios de máquinas locales o remotas, hacer uso de herramientas para el rastreo de vulnerabilidades o para obtener privilegios en equipos de cómputo no otorgados explícitamente por la DTIP.

**ARTÍCULO 24.-** La autenticación del acceso a los Servidores o equipo de cómputo a nivel de sistema operativo donde residan los sistemas y aplicaciones de las dependencias municipales, seguirá las siguientes políticas:

* 1. Para acceder a los servidores a nivel sistema operativo se deberá realizar mediante un proceso de autenticación, el cual podrá realizarse mediante los siguientes métodos: login-password, tokens, sistemas biométricos o cualquier otro análogo a la necesidad, dependiendo del nivel de seguridad requerido;
  2. La contraseña deberá contar con al menos 8 caracteres alfanuméricos;
  3. El acceso de manera remota a los servidores Window s, Linux, Unix o cualquier otro, se realizará por medio de un login y un password, a través de un servicio seguro como ssh (secure Shell) y para transferencia de archivos sftp (secure file transfer protocol); y
  4. Solo estarán disponibles los servicios de red utilizados por el servidor, dejando a los demás servicios inhabilitados. Siendo un ejemplo de ello los servicios web donde solo deberá estar disponible el servicio http y https.

**ARTÍCULO 25.-** Además de lo ya previsto en este apartado, el Área de la DTIP por conducto del área de Redes y Soporte Técnico complementará las medidas de seguridad complementaria con las siguientes acciones:

1. Eliminar de los equipos, los servicios de red que no sean utilizados, tales como protocolos, servicios, opciones, parámetros y utilerías que no se requieran;
2. Evaluar periódicamente los mecanismos de seguridad que protegen el acceso a los equipos de cómputo, servidores y dispositivos de interconexión, a fin de prevenir y detectar riegos de violación a la seguridad de la información y equipos;
3. Prohibir el uso de módems, switches, routers, puentes de acceso inalámbrico y cualquier otro medio ajeno a la infraestructura de cómputo y telecomunicación, para acceder a equipos, aplicaciones, servicios, conexión de red, y demás herramientas cuyo acceso tenga la calidad de restringido;
4. El área de Redes y Soporte Técnico será el responsable de mantener actualizadas y habilitadas permanentemente las herramientas oficiales de protección y limpieza de malware;
5. En aquellos casos de excepción, donde el área de Redes y Soporte Técnico, haya otorgado temporalmente claves de acceso remoto, el área correspondiente deberá vigilar que tenga instaladas las herramientas de protección y limpieza de malware.
6. Someter a pruebas de seguridad todas las aplicaciones que se desarrollen por el área de Ingeniería de Software, antes de ser liberadas y puestas en operación;
7. El usuario que haga uso de programas gestores de descarga, túneles, proxy o cualquier software que intente evadir la seguridad de la red, será sujeto de las medidas disciplinarias correspondientes;
8. En los supuestos de detección de ataque a la red de comunicaciones o cuando se detecte la operación anómala de algún software, proceso, programa o código, así como la presencia de algún virus informático que ponga en riesgo los activos de TIC propiedad de la institución, el área de Redes y Soporte Técnico, realizará las acciones técnicas requeridas para impedir que dichas amenazas ocasionen o pongan en riesgo los recursos tecnológicos institucionales, para tales casos se aplicara el plan de contingencia;
9. En los servidores, se creará una estructura estandarizada de directorios. Los archivos, programas y formatos que integran las aplicaciones, deberán estar instalados en los directorios específicos, que faciliten su operación por parte del personal asignado a las tareas de seguridad, protección y mantenimiento, mismos que contarán con contraseñas específicas para estas tareas;
10. Las contraseñas de los equipos de Telecomunicaciones, Centro de datos y aparatos de infraestructura e interconexión, serán cambiadas periódicamente. La duración de dichas contraseñas tendrá una vigencia de 30 días;
11. El cambio o renuncia de los servidores públicos involucrados en el mantenimiento y soporte de servidores, telecomunicaciones y aparatos de infraestructura será motivo para que las contraseñas de dichos aparatos se cambie inmediatamente a la separación o cambio; y
12. El cambio, asignación, cancelación de contraseñas de Root, Administrador, System, Sistema, Administrador y demás equipos son de uso exclusivo del área de Redes y Soporte Técnico

# CAPÍTULO QUINTO SANCIONES

**ARTÍCULO 26.-** La Contraloría Municipal podrá sancionar de acuerdo a las disposiciones legales aplicables a los servidores públicos de las diferentes áreas o dependencias del Ayuntamiento, cuando se presenten las siguientes causas:

1. Cuando una dependencia se niegue a cooperar en el levantamiento de inventarios de los equipos de cómputo;
2. Cuando se dé un mal uso de los equipos de cómputo;
3. Ocasione una descompostura no aplicable al desgaste natural;
4. Cuando se utilice el equipo de cualquier dependencia, para desarrollar programas, proyectos o trabajos ajenos al interés municipal, así como el uso del servicio con fines partidistas o de lucro;
5. Cuando se reubiquen o muevan los equipos y no respeten las disposiciones de uso y espacios del mismo;
6. Cuando se instale software sin licencia o sin previa autorización del Titular de la DTIP en los equipos de cómputo asignados.
7. Cuando personal no autorizado modifique las configuraciones establecidas por la DTIP para la infraestructura de TIC, puntos de acceso, switches y demás equipo tecnológico del Ayuntamiento
8. Todos los estudios relativos a la topología de redes de comunicaciones, tanto internas como externas, como de los sistemas computacionales, sus esquemas particulares y sus configuraciones de interconexión, son información confidencial. Por lo anterior, cualquier usuario que divulgue por cualquier medio todo o parte de dicha información, se hará acreedor a las sanciones que señale este reglamento y la ley correspondiente.

**ARTÍCULO 27.-** Para efectos del presente reglamento queda estrictamente prohibido:

1. Descargar, copiar o alternar software, no autorizados o sin licencia de dudosa procedencia, que ponga en riesgo el equipo o la red de la Dependencia. Asimismo fotografías, video, o música del Internet; se deberá revisar con antivirus efectivo, cualquier programa o archivo que haya sido descargado y estar completamente seguro que no representa un peligro para el equipo o la red;
2. Utilizar el servicio de conversaciones mediante la red o mensajeros que no sea el institucional;
3. Utilizar el servicio de internet con un fin distinto al de la actividad propia de la Dependencia o encomendado al usuario;
4. Visitar sitios de Internet, en los cuales existan contenidos pornográficos o expresen violencia y maltrato en contra de grupos vulnerables, así como animales u otros que denigren la imagen del Municipio de Atlixco, Puebla y del servidor público;
5. El envío de mensajes en cadena;
6. Enviar mensajes de correo con anexos grandes (mayores a 1MB) a múltiples personas dentro de la Red Interna, cuando sea necesario enviar una notificación de este tipo, deberá solicitarse al administrador del correo electrónico para que genere el mensaje y almacene una copia común de la información en un repositorio general o en algún apartado de la Intranet institucional;
7. Bajar programas de tipo freeware o shareware;
8. Inseminar virus u otro tipo de programas dañinos para sistemas de proceso de la información, con el fin de afectar los datos o registros de otros usuarios;
9. Utilizar los medios de la red con fines ilícitos, de propaganda, comercial, electoral, religiosa, entre otros;
10. Ejecutar juegos interactivos y de azar a través de la Internet Institucional;
11. Ceder o prestar el servicio de Internet Institucional a usuarios de otra oficina que no cuenten con el acceso al mismo, así como a personas ajenas a la institución gubernamental;
12. Transferir o ejecutar archivos o programas no propios del trabajo, que provoquen congestionamiento en los enlaces de comunicación o sistemas informáticos; y
13. Cualquier otro uso no previsto en los presentes lineamientos que no esté orientado.

**ARTÍCULO 28.-** La inobservancia a lo dispuesto en el presente Reglamento motivará la aplicación de sanciones, considerando ante todo la gravedad del hecho constitutivo de la infracción, de sus consecuencias, así como la intencionalidad y reincidencia de la infracción, siendo las siguientes:

1. Por el uso inmoderado del audio en equipo de cómputo, la sanción comprenderá apercibimiento en primera instancia, amonestación por escrito y hasta el retiro de dispositivo de salida de audio del área de trabajo, en caso de reincidir;
2. Por daños intencionales al equipo de cómputo, la sanción comprenderá la reparación del daño ocasionado al componente o equipo, según el valor determinado por el avalúo correspondiente;
3. Por uso de software no autorizado, al responsable se le desinstalará este mismo y se le apercibirá por escrito en primera instancia;
4. Abrir páginas de Internet notoriamente restringidas y hacer mal uso de las claves de acceso y de la RED informática. En caso de reincidencia, se le instaurará Procedimiento administrativo de destitución del cargo desempeñado;
5. Sustraer información confidencial y restringida, mediante cualquier dispositivo de almacenamiento o de cualquier otra naturaleza, sin la autorización correspondiente, al responsable se le impondrá la sanción establecida en la Fracción IV de este artículo;
6. Para las personas que tengan la calidad de visitantes, y se les permita el acceso a la RED informática y que incurran en alguno de los supuestos anteriores, la sanción consistirá en la restricción de acceso a la RED, suspensión temporal o definitiva del permiso de acceso.

Tratándose de daños a los equipos de cómputo o infraestructura, en la reparación del mismo según el avalúo correspondiente;

1. El servidor público que tenga a su cargo un equipo de cómputo y lo preste a personas ajenas a la institución y que haga mal uso del mismo o sustraiga información del mismo, se le impondrá la sanción prevista en la Fracción IV de este artículo; y
2. Las acciones u omisiones no previstas en el presente reglamento, se atenderá a lo establecido en la Ley de Responsabilidades de los

Servidores Públicos del Estado de Puebla y sus Municipios, sin perjuicio de las acciones legales que procedan.

# TRANSITORIOS

**ARTÍCULO PRIMERO.-** El presente Reglamento de la Dirección de Tecnologías de Información y Padrones del Honorable Ayuntamiento de Atlixco, Puebla, entrará en vigor al momento de su publicación en la Gaceta Municipal del H. Ayuntamiento Constitucional o en el Portal Web Institucional de Atlixco, Puebla.

**ARTÍCULO SEGUNDO.-** A partir de la entrada en vigor del presente ordenamiento se deberá capacitar a los servidores públicos del Municipio de Atlixco, para la debida aplicación del Reglamento de la Dirección de Tecnologías de Información y Padrones del Honorable Ayuntamiento de Atlixco, Puebla.

**ARTÍCULO TERCERO.-** Se derogan todas aquellas disposiciones normativas que se opongan al presente Reglamento de la Dirección de Tecnologías de Información y Padrones del Honorable Ayuntamiento de Atlixco, Puebla.