**INDICE**

**EL CONCEJO MUNICIPAL**
**DEL**
**GOBIERNO AUTÓNOMO DESCENTRALIZADO**
**MUNICIPAL DEL CANTÓN ATACAMES**

**EXPIDE:**

**REGLAMENTOS, POLÍTICAS Y PROCEDIMIENTOS DE LA JEFATURA DE SISTEMAS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN ATACAMES**

## JEFATURA DE SISTEMAS

### CAPITULO I

### MISIÓN, VISIÓN Y OBJETIVOS

**ARTICULO 1. MISIÓN.** Gestionar eficiente y eficazmente los recursos, la infraestructura y servicios tecnológicos institucionales, mediante la administración, mantención y desarrollo de sistemas de información y servicios informáticos que apoyen los procesos realizados por usuarios internos y la realización de trámites y obtención de servicios por parte de usuarios externos.

**ARTICULO 2. VISIÓN.** Ofrecer tecnología de punta que ayude a optimizar los procesos que se lleven a cabo en la municipalidad.

**ARTICULO 3. OBJETIVOS.** Proveer de las herramientas tecnológicas necesarias para ejecutar adecuadamente su labor y responder oportunamente a sus necesidades, la jefatura de Sistemas municipal tiene como principal objetivo crear herramientas eficientes, con las cuales garantice la modernidad y la transparencia con las que se rige el Gobierno Municipal.

Proporcionar un buen servicio y adecuado manejo de los equipos existentes.

Desarrollar y mantener sistemas de información que incorporen herramientas que apoyen la ejecución y gestión de los procesos internos.

Implementar y gestionar una plataforma tecnológica que permita proveer servicios informáticos de alta disponibilidad, seguridad y confiabilidad.

Gestionar y mantener servicios de soporte técnico para usuarios internos que permitan mantener la continuidad operativa de su equipo y servicios tecnológicos.

### CAPITULO II

### DISPOSICIONES GENERALES

**ARTICULO 4. ÁMBITO DE APLICACIÓN Y FINES**

**4.1** Las políticas, procedimientos y reglamento son de observación obligatoria para todos los funcionarios que tengan relación laboral dentro del Gobierno autónomo descentralizado del cantón Atacames

**4.2** Las políticas, procedimientos y reglamento de seguridad en la jefatura de Sistemas tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes) y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios que utilicen los equipos de computación y los sistemas del Gobierno Autónomo Descentralizado del Cantón Atacames.

**4.3** La jefatura de Sistemas dará a conocer estas políticas, procedimientos y reglamento de seguridad internamente a todos las unidades del Gobierno Autónomo Descentralizado del Cantón Atacames.

**4.4** La jefatura de Sistemas puede agregar guías particulares complementarias de acuerdo a su naturaleza y funciones. Además será el responsable de hacer cumplir las políticas, procedimientos y reglamento.

**ARTICULO 5. HORARIOS DE TRABAJO**

**5.1** El horario de entrada y salida de los funcionarios se detalla a continuación:

| DIAS LABORABLES DE LUNES A VIERNES | | |
|---|---|---|
| **MAÑANA** | **HORA DE ALMUERZO** | **TARDE** |
| **08:00 am. A 12:30 pm** | **12:30 am. A 13:30 pm.** | **13:30 pm. A 17:00 pm** |

**5.2** Queda prohibido el ingreso y utilización de los equipos y sistemas de información a los funcionarios de la municipalidad fuera del horario de trabajo.

**5.3** Podrán acceder a utilizar los equipos y sistemas de información, siempre y cuando tengan una autorización de la máxima autoridad o el jefe o director de su unidad.

**ARTÍCULO 6. FRECUENCIA DE EVALUACIÓN DE LAS POLÍTICAS.**

**6.1** Se evaluarán las políticas, procedimientos y reglamento del presente documento, con una frecuencia trimestral por el director o jefe encargado de la unidad.

**6.2** Las políticas, procedimientos y reglamento serán evaluadas por la jefatura de sistemas con una frecuencia semestral.

## CAPITULO III

## POLÍTICAS DE SEGURIDAD FÍSICA

**ARTÍCULO 7. ACCESO FÍSICO**

**7.1** Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo. Entendiendo por sistema de comunicaciones: el equipo activo y los medios de comunicación.

**7.2** El acceso de terceras personas debe ser identificado plenamente, controlado y vigilado durante el acceso portando una identificación que les será asignado por el área de seguridad de acceso al edificio.

**7.3** Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área o con permiso del Jefe o Director del Área.

**7.4** Las visitas a las instalaciones físicas de los centros de cómputo, laboratorios o salas de videoconferencia se harán en el horario establecido y cumpliendo lo estipulado en el artículo 7.3.

**7.5** El personal autorizado para mover, cambiar o extraer equipo de cómputo del GADMA es la jefatura de sistemas, el cual notificará al Departamento de Bodega y al personal de seguridad.

**7.6** Todo funcionario y visitante que utilice la infraestructura informática del municipio tal como: equipos de cómputo, sistemas de información, internet, red de voz, datos y programas que son propiedad del GADMA, se obliga a cumplir con las siguientes políticas, procedimiento y reglamentos:

- Solicitar la autorización correspondiente para ingresar equipo de cómputo a la municipalidad.
- Registrar todo equipo de cómputo para su ingreso a la municipalidad a los guardias de seguridad.
- Registrar en vigilancia todo dispositivo de almacenamiento de información a utilizar para su ingreso a la municipalidad.
- Los equipos de cómputo ingresados a la municipalidad, deberán sujetarse a las políticas de seguridad de la municipalidad.
- Contar con un antivirus actualizado.
- Sujetarse a las reglas de acceso a internet controladas por el dispositivo de seguridad configurado en la red.
- Sujetarse a las reglas de acceso a la información controladas por las cuentas asignadas para ello.
- Se deberá reportar en el departamento de sistemas todo equipo de cómputo o dispositivo magnético para su revisión antes de autorizar su salida de la municipalidad.

## ARTÍCULO 8. ROBO DE EQUIPO

**8.1** A partir de los procedimientos definidos por el GADMA, el Departamento de Bodega definirá procedimientos para inventario físico, entregara actas de responsabilidades del equipo de tecnología de información entregado al funcionario.

**8.2** El resguardo de los equipos de comunicaciones deberá quedar asignado a las personas que los usan o administran, permitiendo conocer siempre la ubicación física de los equipos.

**ARTÍCULO 9. PROTECCIÓN FÍSICA**

**9.1** Las puertas de acceso a las salas de cómputo deben ser preferentemente de vidrio transparente, para favorecer el control del uso de los recursos de cómputo.

**9.2** La jefatura de sistemas del GADMA debe:

- Recibir limpieza al menos una vez por semana, que permita mantenerse libre de polvo.
- Ser un área restringida.
- Estar libre de contactos e instalaciones eléctricas en mal estado
- Contar por lo menos con dos extinguidores de incendio adecuado y cercano a la jefatura de sistemas.

**9.3** La jefatura de sistemas deberá seguir los estándares vigentes para una protección adecuada de los equipos y servidores.

**9.4** Para el cuidado de los equipos de cómputo, la municipalidad deberá adecuar las oficinas con muebles que permitan una mejor protección a los mismos (agua, polvo, humedad, etc).

**9.5** Los departamentos de la municipalidad deberán estar en un buen ambiente de ventilación para proteger a los equipos de cómputo.

**9.6** Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas de la jefatura de sistemas deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.

**9.7** Cada vez que se requiera conectar equipo de cómputo, se deberá comprobar la carga de las tomas de corriente.

**9.8** Las instalaciones eléctricas deberán estar en continuo mantenimiento por el área encargada, para garantizar la protección de los equipos de cómputo.

**9.9** Se deberá tener fácil acceso a los procedimientos de contingencias.

**ARTÍCULO 10. RESPALDOS**

**10.1** Las Bases de Datos de los sistemas del GADMA serán respaldadas periódicamente en forma automática y manual, según los procedimientos generados para tal efecto.

**10.2** Los respaldos de los sistemas del GADMA deberán ser almacenados en un lugar seguro y distante del sitio de trabajo.

**10.3** Los funcionarios serán responsables del respaldo de la información de su equipo asignado, de acuerdo a las recomendaciones del departamento de TII.

**10.4** Para una mejor protección de los respaldos de información de cada servidores información de cada equipo de cómputo serán guardados en la nube.

## CAPITULO IV
## POLÍTICAS DE SEGURIDAD LÓGICA DE LA RED DEL GADMA

### ARTÍCULO 11. DE LA RED

**11.1** La Red del GADMA tiene como propósito principal servir en la transformación e intercambio de información dentro de la entidad entre usuarios, técnicos, departamentos, oficinas y hacia a fuera de la entidad con otros puertos entre éstas y otros servicios locales, nacionales e internacionales, a través de conexiones con otras redes.

**11.2** Si una aplicación en la red es coherente con los propósitos de la Red del GADMA, entonces significa que las actividades necesarias para esa aplicación serán consistentes con los propósitos de la jefatura de sistemas.

**11.3** La jefatura de sistemas no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.

**11.4** Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.

**11.5** No se permite interferir o interrumpir las actividades de los demás usuarios por cualquier medio o evento salvo que las circunstancias así lo requieran, como casos de contingencia, los cuales deberán ser reportados en su momento a sus superiores correspondientes.

**11.6** No se permite el uso de los servicios de la red cuando no cumplan con los trabajos propios del GADMA.

**11.7** Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad del GADMA y se usarán exclusivamente para actividades relacionadas con el municipio.

**11.8** Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.

**11.9** El uso de analizadores de red es permitido única y exclusivamente por el personal de la jefatura de sistemas, para monitorear la funcionalidad de la Red del GADMA, contribuyendo a la consolidación del sistema de seguridad bajo las políticas y normatividades del GADMA.

**11.10** No se permitirá el uso de analizadores para monitorear o censar redes ajenas al GADMA y no se deberán realizar análisis de la Red del GADMA desde equipos externos a la entidad.

**11.11** Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red involucrada dependiendo de la normatividad. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

**11.12** Para el control y la seguridad de la red telefónica interna se llevara un monitoreo del funcionamiento.

**11.13** Se crearan políticas de acceso y uso de la red Wifi de la municipalidad.

**11.14** Se crearan políticas establecidas en el equipo firewall, para un mejor control de seguridad en los equipos de la municipalidad.

### ARTÍCULO 12. LA JEFATURA DE SISTEMAS

**12.1** La jefatura de sistemas debe llevar un control total y sistematizado de los recursos de cómputo.

**12.2** Los encargados de la jefatura de sistemas son los responsables de hacer el calendario y organizar al personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo.

**12.3** Los Jefes y Directores deberán reportar al personal de la jefatura de sistemas cuando el usuario deje de laborar o de tener una relación con la municipalidad.

**12.4** Si un usuario o departamento viola las políticas vigentes de uso aceptable de la Red del GADMA, los administradores de la Red lo aislará de la misma.

**12.5** Para reforzar la seguridad de la información de los usuarios, bajo su criterio, deberá hacer respaldos de la información en sus discos duros dependiendo de la importancia y frecuencia del cambio de la misma.

**12.6** Los administradores no podrán remover del sistema ninguna información de cuentas individuales, a menos que la información sea de carácter ilegal, o ponga en peligro el buen funcionamiento de los sistemas, o se sospeche de algún intruso utilizando una cuenta ajena.

**12.7** La jefatura de sistemas es el responsable del control y operatividad de manejo de la red telefónica interna.

**12.8** La jefatura de sistemas es la encargada de habilitar o bloquear las llamadas (local, nacional o celular), con la autorización de la Dirección Administrativa, pasando un informe de acuerdo a la actividad según el departamento, para poder llevar un control de consumo telefónico.

**12.9** La jefatura de sistemas llevara un control de monitoreo e inspecciones constantes a los equipos conectados en la red Wifi de la municipalidad, ya sean estos propios o ajenos a la misma.

**12.10** La jefatura de sistema establecerá políticas y monitoreara los equipos y recursos tecnológicos a través de firewall.

**12.11** La jefatura de sistemas dará a la Dirección Administrativa reportes estadísticos de recursos consumidos en la red.

**ARTÍCULO 13. POLÍTICAS DE USO ACEPTABLE DE LOS FUNCIONARIOS**

**13.1** Los recursos de cómputo empleados por el funcionario:

- Deberán ser afines al trabajo desarrollado.
- No deberán ser proporcionados a personas ajenas.
- No deberán ser utilizados para fines personales.

**13.2** Todo usuario debe respetar la intimidad, confidencialidad y derechos individuales de los demás usuarios.

**13.3** Es responsabilidad del usuario, hacer buen uso del equipo de Cómputo Asignado, así como la conservación, integridad y contenidos de la información que se encuentre en los discos duros de los equipos de escritorios y portátiles.

**13.4** El correo electrónico no se deberá usar para envío masivo, materiales de uso no institucional o innecesarios (entiéndase por correo masivo todo aquel que sea ajeno a la institución, tales como cadenas, publicidad y propaganda comercial, política o social, etcétera).

**13.5** Para reforzar la seguridad de la información de su cuenta, el funcionario conforme su criterio deberá hacer respaldos de su información, dependiendo de la importancia y frecuencia de modificación de la misma. Los respaldos serán responsabilidad absoluta de los funcionarios.

**13.6** Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor, para tal efecto todos los funcionarios deberán firmar un manifiesto donde se comprometan, bajo su responsabilidad, a no usar programas de software que violen la ley de derechos de autor.

**13.7** Los funcionarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y red del GADMA, de acuerdo con las políticas que en este documento se mencionan.

**13.8** Los funcionarios deberán solicitar apoyo a la jefatura de sistemas ante cualquier duda en el manejo de los recursos de cómputo de la institución.

**13.9** El uso de los teléfonos asignados al departamento deberán ceñirse a las actividades relacionadas del departamento, en caso del no cumplimiento de acuerdo a sus actividades de uso, se informara a la Dirección Administrativa para su bloqueo.

**ARTÍCULO 14. DE LOS SERVIDORES DE LA RED DEL GADMA.**

**14.1** La jefatura de sistemas tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.

**14.2** La instalación y/o configuración de todo servidor conectado a la Red será responsabilidad de la jefatura de Sistemas.

**14.3** Durante la configuración del servidor la jefatura de sistemas deben normar el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.

**14.4** Queda estrictamente prohibido acceder a sitios:

- Redes sociales y mensajería instantánea.
- pornografía.
- Descarga de música en su diversos formatos: Mp3, RA, CDA etc.
- Descarga de video en su diversos formatos.
- Escuchar la radio y ver televisión por Internet. Salvo en aquellos casos que se justifique, contando con el visto bueno del jefe o director de área correspondiente o tal caso de la máxima autoridad.
- Demás sitios que sean distractores de las actividades propias del puesto.

**14.5** Los servidores que proporcionen servicios a través de la RED e Internet deberán:

- Funcionar 24 horas del día los 365 días del año, a exención de los mantenimientos planificados y caso fortuitos (falla energía, incendio o desastres naturales).
- Recibir mantenimiento preventivo máximo dos veces al año
- Recibir mantenimiento semestral que incluya depuración.
- Recibir mantenimiento anual que incluya la revisión de su configuración.
- Ser monitoreados por la jefatura de sistemas de la entidad y por el Centro de Operaciones de la Red del GADMA.

**14.6** La información de los servidores deberá ser respaldada de acuerdo con los siguientes criterios, como mínimo:

- Diariamente, información crítica.
- Semanalmente, los correos y los documentos web.
- Mensualmente, configuración del servidor.

**14.7** Los servicios institucionales hacia Internet sólo podrán proveerse a través de los servidores autorizados por la jefatura de sistemas.

**14.8** La Jefatura de Sistemas se encargará de asignar las cuentas a los usuarios para el uso de correo electrónico en los servidores que administra.

**14.9** Para efecto de asignarle su cuenta de correo al usuario, éste deberá llenar una solicitud en formato libre y entregarlo al área de sistemas, con su firma y la del Jefe o Director del área.

**14.10** Una cuenta deberá estar conformada por la primera letra de su nombre y apellido del funcionario y su contraseña asignada. La sintaxis de la cuenta de correo será lquintero@municipiodeatacames.gob.ec y no deberá contener alias.

**14.11** La cuenta será activada en el momento en que el funcionario esté presente en su lugar de trabajo con su máquina asignada por bodega, para que verifique de manera personal su contraseña de acceso.

**14.12** Queda terminantemente prohibido el uso del correo personal para el manejo de información de la institución, se deberá utilizar el correo institucional para el envío y recepción de información interna o externa.

**14.13** Los servidores deberán ubicarse en un área física que cumpla las normas:

- Acceso restringido.
- Temperatura adecuada al equipo.
- Protección contra descargas eléctricas.
- Mobiliario adecuado que garantice la seguridad de los equipos.

**14.14** En caso de olvido de la contraseña por parte del usuario, podrá apoyarse con la jefatura de sistemas para el cambio de contraseña.

**14.15** Los funcionarios de red, están sujetos a cumplir las siguientes políticas, procedimientos y reglamento de seguridad:

- Es responsable del uso de su cuenta de red. No compartir sus contraseñas de acceso a la red.
- No dejar sesiones de red abiertas con su cuenta.
- Mantener su equipo de cómputo bloqueado cada vez que se ausente de él por periodos prolongados.
- Almacenar toda la información generada en la carpeta asignada dentro del servidor para garantizar el respaldo de la misma.
- Queda prohibido realizar cualquier tipo de instalación de programas.
- La información almacenada en el equipo deberá estar disponible en todo momento para su auditoría, toda vez que esta requiera, es propiedad de la institución.
- Queda prohibida la ejecución de cualquiera de los siguientes programas sin la autorización y solicitud correspondiente:
  - Programas peer to peer para descarga de archivos
  - Programas de descarga por torrent
  - Juegos
  - Programas de chat
  - Programas que modifiquen la apariencia, colores e íconos del sistema operativo.
  - Screen savers no provistos por la jefatura de sistemas.
  - Queda prohibido descargar correos de buzones con cuentas personales o ajenas a la institución sin la autorización y solicitud correspondiente.
  - Estrictamente prohibido conectar a la red de la municipalidad dispositivos de almacenamiento magnético personales sin autorización, tales como:
    - ✓ Pcs, Notebook
    - ✓ Pda, palm
    - ✓ Smarthphone personal
    - ✓ Usb personal
    - ✓ Blackberry personal
    - ✓ Disco duros externos
    - ✓ Cd o disquete regrabable
- Toda información generada o consultada con algún recurso informático de la institución, queda a disposición de ser auditada, revisada por la Municipalidad.
- Procurar en todo momento mantener la seguridad de la información ya que es propiedad de la municipalidad.

**ARTÍCULO 15. DE LOS SISTEMAS INSTITUCIONALES DE INFORMACIÓN**

**15.1** El ABD tendrá acceso a la información de la Base de Datos únicamente para:

- La realización de los respaldos de la BD.
- Solucionar problemas que el funcionario no pueda resolver.
- Diagnóstico o monitoreo.

**15.2** El Administrador de la Base de Datos no deberá eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema.

**15.3** El Administrador de la Base de Datos es el encargado de asignar las cuentas a los usuarios para el uso. Para tal efecto será necesario seguir el procedimiento determinado.

**15.4** Las contraseñas serán asignadas por el Administrador de la Base de Datos en el momento en que el usuario desee activar su cuenta, previa solicitud del jefe o director de acuerdo con el procedimiento generado.

**15.5** En caso de olvido de contraseña de un usuario, será necesario que se presente con el Administrador de la Base de Datos para reasignarle su contraseña.

## CAPITULO V

## POLÍTICAS DE ADQUISICIÓN DE EQUIPOS TECNOLÓGICOS

### ARTÍCULO 16. EQUIPOS TECNOLÓGICOS NUEVOS

**16.1** El departamento de TII será el encargado de dar la asesoría con las especificaciones técnicas para la adquisición de los nuevos equipos tecnológicos.

**16.2** Todo departamento que requiera realizar una adquisición de un equipo tecnológico, pedirá la asesoría al departamento de TII.

**16.3** Los equipos que se adquieran de manera arbitraria y no cumplan con los fines de acuerdo al trabajo a realizar, sin asesoría del departamento de TII, será responsabilidad del departamento que realizo el requerimiento.

**16.4** El departamento de TII será el responsable de asignar los equipos, para aprovechar los recursos tecnológicos de acuerdo a la función que cada usuario realice por departamento.

## CAPITULO VI

## POLÍTICAS DE SEGURIDAD LÓGICA PARA ADMINISTRACIÓN DE LOS RECURSOS DE CÓMPUTO

### ARTÍCULO 17. ÁREA DE SEGURIDAD EN CÓMPUTO

**17.1** La jefatura de Sistemas es el encargado de suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad en cómputo. Sin embargo, debido a la cantidad de usuarios y a la amplitud y constante innovación de los mecanismos de ataque no es posible garantizar una seguridad completa.

**17.2** La jefatura de Sistemas debe mantener informados a los funcionarios y poner a disposición de los mismos el software que refuerce la seguridad de los sistemas de cómputo.

**17.3** La jefatura de Sistemas es el único autorizado para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios de la Red.

### ARTÍCULO 18. ADMINISTRADORES DE TECNOLOGÍAS DE INFORMACIÓN.

**18.1** Los ATI deben cancelar o suspender las cuentas de los usuarios previa notificación, cuando se le solicite mediante un documento explícito por el Jefe o Director del área en los siguientes casos:

- ❖ Si la cuenta no se está utilizando con fines institucionales.
- ❖ Si pone en peligro el buen funcionamiento de los sistemas.
- ❖ Si se sospecha de algún intruso utilizando una cuenta ajena.

**18.2** El ATI deberá ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del propietario de la computadora.

**18.3** El ATI deberá utilizar los analizadores previa autorización del funcionario y bajo la supervisión de éste, informando de los propósitos y los resultados obtenidos.

**18.4** El ATI deberá realizar respaldos periódicos de la información de los recursos de cómputo que tenga a su cargo, siempre y cuando se cuente con dispositivos de respaldo.

**18.5** El ATI debe actualizar la información de los recursos de cómputo de la entidad, cada vez que adquiera e instale equipo o software.

**18.6** El ATI debe registrar cada máquina en el inventario de control de equipo de cómputo y red de la entidad.

**18.7** El ATI debe auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.

**18.8** EL ATI debe realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo con los requerimientos en materia de seguridad.

**18.9** Es responsabilidad del ATI revisar periódicamente los sistemas a su cargo.

**18.10** EL ATI reportará a la Jefatura o Dirección los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

**ARTÍCULO 19. RENOVACIÓN DE EQUIPO**

**19.1** Se deberán definir los tiempos estimados de vida útil de los equipos de cómputo para programar con anticipación su renovación.

**19.2** Para la adquisición de equipo de cómputo se deberá cumplir con lo establecido en la Ley de Adquisiciones así como el Decreto Presidencial para el uso racional de los recursos de TI.

**19.3** Cuando las áreas requieran de un equipo para el desempeño de sus funciones ya sea por sustitución o para el mejor desempeño de sus actividades, estas deberán realizar una consulta al ATI a fin de que se seleccione el equipo adecuado. Sin el Visto Bueno de la jefatura de sistemas no se podrá hacer la adquisición de compra de TIC o de equipos.

## CAPÍTULO VII
## POLÍTICAS DE SEGURIDAD LÓGICA PARA EL USO DE SERVICIOS DE RED

**ARTÍCULO 20. SERVICIOS A LAS JEFATURAS Y DIRECCIONES**

**20.1** Los Jefes o Directores definirán los servicios de Internet a ofrecer a los funcionarios a su cargo y se coordinará con el ATI para su otorgamiento y configuración.

**20.2** Los Jefes o Directores pueden utilizar la infraestructura de la Red para proveer servicios a los usuarios externos y/o visitas previa autorización de la jefatura de Sistemas.

**20.3** El ATI es el responsable de la administración de contraseñas y deberá guardar su confidencialidad, siguiendo el procedimiento para manejo de contraseñas.

**20.4** No se darán equipo, contraseñas ni cuentas de correo a personas que presten servicio social o estén haciendo prácticas profesionales en la municipalidad.

**20.5** Los Jefes o Directores deberán notificar a la jefatura de Sistemas cuando un usuario deje de prestar sus servicios a la municipalidad.

**20.6** El ATI realizará las siguientes actividades en los servidores de la municipalidad:

- Respaldo de información conforme a los procedimientos indicados por el centro de operaciones.
- Revisión y reporte de cualquier eventualidad al Centro de Operaciones de la RED.
- Implementar de forma inmediata las recomendaciones de seguridad proporcionados y reportar a la Dirección posibles faltas a las políticas de seguridad en cómputo.
- Monitoreo de los servicios de red proporcionados por los servidores a su cargo.
- Calendarizar, organizar y supervisar al personal encargado del mantenimiento preventivo y correctivo de los servidores.

**20.7** El ATI es el único autorizado para asignar las cuentas a los usuarios con previa solicitud de autorización de los Jefes o Directores.

**20.8** La jefatura de Sistemas aislará cualquier servidor de red, notificando a los Jefes o Directores, en las condiciones siguientes:

- Si los servicios proporcionados por el servidor implican un tráfico adicional que impida un buen desempeño de la Red.
- Si se detecta la utilización de vulnerabilidades que puedan comprometer la seguridad en la Red.
- Si se detecta la utilización de programas que alteren la legalidad y/o consistencia de los servidores.
- Si se detectan accesos no autorizados que comprometan la integridad de la información.
- Si se viola las políticas de uso de los servidores.
- Si se reporta un tráfico adicional que comprometa a la red de la municipalidad.

**ARTÍCULO 21. USO DE LOS SERVICIOS DE RED POR LOS FUNCIONARIOS.**

**21.1** El usuario deberá definir su contraseña de acuerdo al procedimiento establecido para tal efecto y será responsable de la confidencialidad de la misma.

**21.2** El usuario deberá renovar su contraseña y colaborar en lo que sea necesario, a solicitud del ATI, con el fin de contribuir a la seguridad de los servidores en los siguientes casos:

- ✓ Cuando ésta sea una contraseña débil o de fácil acceso.
- ✓ Cuando crea que ha sido violada la contraseña de alguna manera.

**21.3** El usuario deberá notificar al ATI en los siguientes casos:

- Si observa cualquier comportamiento anormal (mensajes extraños, lentitud en el servicio o alguna situación inusual) en el servidor.
- Si tiene problemas en el acceso a los servicios proporcionados por el servidor.

**21.4** Si un usuario viola las políticas de uso de los servidores, el ATI podrá cancelar totalmente su cuenta de acceso a los servidores, notificando a la jefatura o dirección correspondiente.

## CAPÍTULO VIII

## POLÍTICAS DE SEGURIDAD LÓGICA PARA EL USO DEL ANTIVIRUS INSTITUCIONAL

### ARTÍCULO 22. ANTIVIRUS DE LA RED

**22.1** Deberán ser utilizadas en la implementación y administración de la Solución Antivirus.

**22.2** Todos los equipos de cómputo del GADMA deberán tener instalada la Solución Antivirus.

**22.3** Periódicamente se hará el rastreo en los equipos de cómputo del GADMA, y se realizará la actualización de las firmas antivirus proporcionadas por el fabricante de la solución antivirus en los equipos conectados a la Red.

**22.4** Por medio de la solución antivirus se bloquearan redes sociales y extensiones de páginas que atenten con la seguridad de la red.

### ARTÍCULO 23. POLÍTICAS ANTIVIRUS.

**23.1** El ATI será el responsable de:

- Implementar la Solución Antivirus en las computadoras de la entidad.
- Solucionar contingencias presentadas ante el surgimiento de virus que la solución no haya detectado automáticamente. Configurar el analizador de red para la detección de virus.

**23.2** El administrador de la Red aislará el equipo o red, notificando a la Jefatura o Dirección correspondiente, en las condiciones siguientes:

- Cuando la contingencia con virus no es controlada, con el fin de evitar la propagación del virus a otros Equipos y redes.
- Si el funcionario viola las políticas antivirus.
- Cada vez que los funcionarios requieran hacer uso de discos, USB's, éstos serán rastreados por la Solución Antivirus en la computadora del usuario o en un equipo designado para tal efecto en las áreas de cómputo de las dependencias.

**23.3** En caso de contingencia con virus el ATI deberá seguir el procedimiento establecido.

### ARTÍCULO 24. USO DEL ANTIVIRUS POR LOS FUNCIONARIOS

**24.1** El funcionario no deberá desinstalar la solución antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus.

**24.2** Si el funcionario hace uso de medios de almacenamiento personales, éstos serán rastreados por la Solución Antivirus en la computadora del usuario o por el equipo designado para tal efecto.

**24.3** El funcionario que cuente con una computadora con recursos limitados, contará con la versión ligera de la Solución Antivirus Institucional.

**24.4** El funcionario deberá comunicarse con el ATI en caso de problemas de virus para buscar la solución.

**24.5** El funcionario será notificado por el ATI en los siguientes casos:

- Cuando sea desconectado de la red con el fin de evitar la propagación del virus a otros usuarios de la dependencia.
- Cuando sus archivos resulten con daños irreparables por causa de virus.
- Cuando violen las políticas antivirus.

## CAPÍTULO IX

## ARTICULO 25. POLÍTICAS DE OPERACIÓN DE LOS CENTROS DE CÓMPUTO

**25.1** La Jefatura de Sistemas podrá ofrecer servicios de cómputo, soporte técnico y servicios audiovisuales en las salas de juntas de la entidad.

**25.2** La Jefatura de Sistemas dará a conocer dicho reglamento mediante diversos mecanismos como pláticas introductorias y la publicación vía Web y la entrega del documento.

**25.3** La administración de los servicios de la Red deberá llevarse a través de métodos automatizados.

**25.4** Los ATI de la Red deberán verificar el grado de seguridad del software adquirido e instalado en los equipos.

**25.5** El personal de la jefatura de sistemas dará soporte técnico únicamente al equipo de cómputo de la entidad.

**25.6** La Jefatura de Sistemas deberá contar con personal para actividades administrativas, para soporte técnico, para administrar

**25.7** La Jefatura de Sistemas deberá contar con servicios automatizados de los recursos de cómputo, desarrollo de aplicaciones, etc.

**25.8** incluya: Mantenimiento preventivo y correctivo al software, publicación de documentos de normatividad, inventario.

**25.9** La Jefatura de Sistemas deberá contar con la siguiente documentación: Información técnica: manuales y procedimientos, normatividad, inventarios de hardware y software, que puedan servir en caso de contingencia.

**25.10** En caso de daño leve en el equipo, el personal de soporte técnico deberá repararlo o de no lograrlo notificará al usuario para que tome las medidas correspondientes, si el equipo se manda a reparación.

**25.11** La instalación de Software específico deberá ser realizada en conjunto y común acuerdo del funcionario que lo solicite y el ATI.

## CAPÍTULO X

## SANCIONES

### ARTÍCULO 26. GENERALES

Cualquier acción que vaya en contra de las políticas de seguridad en cómputo del GADMA debe ser sancionada con la suspensión de los servicios de cómputo y red, por un período determinado por la Jefatura de Sistemas y la Jefatura o Dirección correspondiente, con conocimiento a la Dirección de talento humano en una primera ocasión y de manera indefinida en caso de reincidencia.

## CAPITULO XI

### ARTÍCULO 27. DEFINICIONES

- ✓ **ABD:** Administrador de Base de Datos.
- ✓ **GADMA:** Gobierno Autónomo Descentralizado Municipal del Cantón Atacames
- ✓ **ASC:** Área de Seguridad en Cómputo del (Áreas de seguridad en: Informática, Telemática). Se encarga de definir esquemas y políticas de seguridad en materia de cómputo para la entidad.
- ✓ **ATI:** Administrador de Tecnologías de Información (Telemática). Responsable de la administración de los equipos de cómputo, sistemas de información y redes de telemática de la Entidad.
- ✓ **BD:** Base de datos.
- ✓ **CAV:** Central Antivirus.
- ✓ **Centro de Cómputo:** Cualquier oficina que cuenten con equipamiento de cómputo.
- ✓ **Centro de Operaciones de la Red:** Es el área que se encarga del funcionamiento y operación de las Tecnologías de Información y comunicaciones (Telemática) en el GADMA.
- ✓ **Contraseña:** Conjunto de caracteres que permite el acceso de un usuario a un recurso informático (password).
- ✓ **Recurso informático:** Cualquier componente físico o lógico de un sistema de información.
- ✓ **Red:** Equipos de cómputo, sistemas de información y redes de telemática del GADMA.
- ✓ **SII:** Sistema Integral de Información del GADMA..
- ✓ **Site:** Espacio designado en la entidad a los equipos de telecomunicaciones y servidores.
- ✓ **Solución Antivirus:** Recurso informático empleado en el GADMA para solucionar problemas causados por virus informáticos.
- ✓ **Telemática:** Conjunto de servicios y técnicas que asocian las telecomunicaciones y la informática ofreciendo posibilidades de comunicación e información.
- ✓ **TIC:** (Tecnologías de Información y Comunicaciones) conjunto de teorías y de técnicas que permiten el aprovechamiento práctico de la Información.
- ✓ **Usuario:** Cualquier persona (empleado o no) que haga uso de los servicios de las tecnologías de información proporcionadas por el GADMA tales como equipos de cómputo, sistemas de información, redes de telemática.
- ✓ **Virus informático:** Programa ejecutable o pieza de código con habilidad de ejecutarse y reproducirse, regularmente escondido en documentos electrónicos, que causan problemas al

ocupar espacio de almacenamiento, así como destrucción de datos y reducción del desempeño de un equipo de cómputo.

Cualquier reforma o anexo que se incluya en este documento será notificado a la máxima autoridad para su aprobación.

**DEROGATORIA**

**PRIMERA.-** Quedan derogadas todos los reglamentos internos, que se opongan al presente.

**DISPOSICIONES FINALES:**

**Primera**.- El presente Reglamento Interno entrará en vigencia a partir de su aprobación por el Gobierno Autónomo Descentralizado Municipal del Cantón Atacames.

Publíquese el presente Reglamento Interno en el dominio Web del Gobierno Autónomo Descentralizado Municipal del Cantón Atacames.

Dado y firmado en la Sala de Sesiones del Concejo Municipal del Cantón Atacames, a los 14 días del mes de septiembre del 2018.

Lcdo. Byron Aparicio Chiriboga
**ALCALDE**

Ab. Mónica González Cervantes
**SECRETARIA GENERAL**

**TRÁMITE DE DISCUSIÓN Y APROBACIÓN POR PARTE DEL CONCEJO MUNICIPAL**

Atacames, a los 14 días del mes de Septiembre del 2018.- La infrascrita Secretaria General del Gobierno Autónomo Descentralizado Municipal de Atacames, CERTIFICA que el "**REGLAMENTO, POLÍTICAS Y PROCEDIMIENTOS DE LA JEFATURA DE SISTEMAS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN ATACAMES**". Fue discutido en primer debate en Sesión ordinaria del 4 de septiembre del 2018, y en segundo debate en Sesión Ordinaria del 14 de septiembre del 2018. LO CERTIFICO.-

Ab. Mónica González Cervantes
**SECRETARIA GENERAL**
**GOBIERNO AUTÓNOMO DESCENTRALIZADO**
**MUNICIPAL DE ATACAMES**

**PROCESO DE SANCIÓN**

**SECRETARÍA GENERAL DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE ATACAMES.-** Atacames 17 de septiembre del 2018.- De conformidad con la razón que antecede y en cumplimiento a lo dispuesto en inciso cuarto del Artículo 322 del Código Orgánico de Organización Territorial, Autonomía y Descentralización, remítase al señor Alcalde del Gobierno Autónomo Descentralizado Municipal de Atacames el "**REGLAMENTO, POLÍTICAS Y PROCEDIMIENTOS DE LA**

**JEFATURA DE SISTEMAS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN ATACAMES".** Para la sanción respectiva.

Ab. Mónica González Cervantes
**SECRETARIA GENERAL**
**GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE ATACAMES**

GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DE ATACAMES
SECRETARIA GENERAL

**SANCIÓN**

**ALCALDÍA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE ATACAMES.-** Atacames 17 de septiembre del 2018.- De conformidad con la disposición contenida en el cuarto inciso del artículo 322 del Código Orgánico de Organización Territorial, Autonomía y Descentralización, habiéndose observado el trámite legal y estando de acuerdo con la Constitución de la República del Ecuador, **SANCIONO** el "**REGLAMENTO, POLÍTICAS Y PROCEDIMIENTOS DE LA JEFATURA DE SISTEMAS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN ATACAMES",** además dispongo la promulgación y publicación, de acuerdo al artículo 324 del Código Orgánico de Organización Territorial, Autonomía y Descentralización

Lcdo. Byron Aparicio Chiriboga
**ALCALDE**
**GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE ATACAMES**

GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DE ATACAMES
ALCALDIA

Proveyó y firmó el señor Licenciado Byron Aparicio Chiriboga, Alcalde del Gobierno Autónomo Descentralizado Municipal de Atacames, el "**REGLAMENTO, POLÍTICAS Y PROCEDIMIENTOS DE LA JEFATURA DE SISTEMAS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN ATACAMES".** Atacames 17 de septiembre del 2018.- LO CERTIFICO.-

Ab. Mónica González Cervantes
**SECRETARIA GENERAL**
**GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE ATACAMES**

GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DE ATACAMES
SECRETARIA GENERAL