EN LA CIUDAD DE ZIHUATANEJO DE AZUETA, GUERRERO, SIENDO LAS **ONCE HORAS** HORAS DEL DIA **TRES** DEL MES DE **ENERO** DEL AÑO **DOS MIL DIECINUEVE**, SE DA INICIO A LA SESION EXTRAORDINARIA DE LA APROBACION DEL MANUAL DE INTEGRACION Y FUNCIONAMIENTO DEL COMITÉ DE TECNOLOGIA DE INFORMACIÓN Y COMUNICACIONES DEL H. AYUNTAMIENTO DE ZIHUATANEJO DE AZUETA, GUERRERO, CELEBRANDOSE EN SALA DE CABILDO DEL H. AYUNTAMIENTO MUNICIPAL CONSTITUCIONAL DE ZIHUATANEJO DE AZUETA, GUERRERO, UBICADAS EN AVENIDA PASEO DE ZIHUATANEJO PONIENTE 21, COLONIA LA DEPORTIVA, PRESIDIENDO LA MISMA EL ING, ADALBERTO TOLEDO SALGADO, EN SU CARÁCTER DE PRESIDENTE DEL COMITÉ DE TECNOLOGIA DE INFORMACIÓN Y COMUNICACIONES, Y CON FUNDAMENTO EN LOS ARTICULOS 115 FRACCION II DE LA CONSTITUCIÓN POLITICA DE LOS ESTADOS UNIDOS MEXICANOS; ARTICULO 178 FRACCIÓN II DE LA CONSTITUCIÓN POLITICA DEL ESTADO LIBRE Y SOBERANO DE GUERRERO; ARTICULO 6 FRACCIÓN V DE LA LEY ORGANICA DEL MUNICIPIO LIBRE DEL ESTADO DE GUERRERO, HACIENDO CONSTAR CON LA ASISTENCIA DE LAS SIGUIENTES **PERSONAS.**- ----------
---

1.- LIC. JORGE SÁNCHEZ ALLEC;	(PRESIDENTE HONORARIO)
2.- ING. ADALBERTO TOLEDO SALGADO	(PRESIDENTE DEL COMITÉ)
3.- LIC. JUAN MANUEL JUAREZ MEZA;	(SECRETARIO TECNICO)
4.- LIC. MARIO MIRANDA FLORES;	(VOCAL)
5.- LIC. LISSETH DE JESÚS GUTIÉRREZ SOLÍS;	(VOCAL)
6.- LIC. ABEL ALCARAZ ALCANTAR;	(VOCAL)
7.- ING. ERICK JAVIER PINEDA SANCHEZ	(VOCAL)
8.- LIC. SALVADOR MELESIO SANDOVAL;	(VOCAL)
9.- L.C. ERIKA VAZQUEZ GARCÍA;	(ASESOR)
10.-LIC. ELADIO MOSQUEDA GONZÁLEZ;	(ASESOR)

ACTO CONTINUO SE PROCEDE AL DESAHOGO DE LA SESION EN LOS SIGUIENTES PUNTOS:

ORDEN DEL DIA:

1.- PASE DE LISTA Y DECLARACIÓN DEL QUORUM;
2.- APROBACIÓN DEL ORDEN DEL DÍA.
3- APROBACION DEL MANUAL DE INTEGRACION Y FUNCIONAMIENTO DEL COMITÉ DE TECNOLOGIA DE INFORMACIÓN Y COMUNICACIONES DEL H. AYUNTAMIENTO DE ZIHUATANEJO DE AZUETA.
4.- APROBACION DEL CALENDARIO DE SESIONES ORDINARIAS PROGRAMADAS DEL COMITÉ DE TECNOLOGIA DE INFORMACIÓN Y COMUNICACIONES.
5.-. CLAUSURA.

SE PROCEDE A DAR LA BIENVENIDA Y PASAR LISTA DE ASISTENCIA, CONTANDOSE CON LA PRESENCIA DE LOS CC. LIC. JORGE SÁNCHEZ ALLEC, PRESIDENTE MUNICIPAL CONSTITUCIONAL DEL H. AYUNTAMIENTO DE ZIHUATANEJO DE AZUETA; ING. ADALBERTO TOLEDO SALGADO, JEFE DE TECNOLOGIAS DE LA INFORMACION; LIC. JUÁN MANUEL JUÁREZ MEZA, SECRETARIO DEL AYUNTAMIENTO; LIC. MARIO MIRANDA FLORES, OFICIAL MAYOR; LIC. LISSETH DE JESÚS GUTIÉRREZ SOLÍS, TESORERA MUNICIPAL; LIC. ABEL ALCARAZ ALCANTAR, DIRECTOR DE PLANEACIÓN Y EVALUACIÓN; ING. ERICK JAVIER PINEDA SANCHEZ, ASESOR TECNICO; LIC. SALVADOR MELESIO SANDOVAL, DIRECTOR DE COMUNICACIÓN; L.C. ERIKA VAZQUEZ GARCÍA, TITULAR DEL ORGANO DE CONTROL INTERNO; LIC. ELADIO MOSQUEDA GONZÁLEZ, DIRECTOR DE ASUNTOS JURIDICOS; POR LO ANTERIOR SE DECLARA LA EXISTENCIA DEL QUORUM LEGAL. PARA SESIONAR, DECLARANDO EL PRESIDENTE INSTALADA Y ABIERTA LA SESION, SIENDO VALIDOS LOS ACUERDOS QUE EN ELLA SE TURNEN.

PROPUESTA.- Y EN SU CASO APROBACION DE LA ORDEN DEL DIA.- POR LO QUE EL PRESIDENTE PONE A CONSIDERACION DE LOS PRESENTES LA ORDEN DEL DIA E INSTRUYE AL SECRETARIO PARA QUE PROCEDA A SOLICITAR POR VOTACION, CONFORME A LA LISTA DE ASISTENCIA POR LO QUE EL SECRETARIO SOLICITA A LOS INTEGRANTES EMITAN SU VOTO PARA LA APROBACION O NO DE LA ORDEN DEL DIA Y MEDIANTE VOTACION ECONOMICA, EL SECRETARIO DECLARA QUE SE APRUEBA POR UNANIMIDAD EL DESARROLLO Y DESAHOGO DE LA SESION CONFORME A LA ORDEN DEL DIA PUESTA A CONSIDERACION.

ACTO SEGUIDO EN DESAHOGO **DE** LA ORDEN DEL DIA APROBADA **SE** DESARROLLA LA SESION EN LOS SIGUIENTES TERMINOS.

PRIMER PUNTO.- LISTA DE FE ASISTENCIA Y DECLARACION DE QUOROM. FUE AGOTADO EN LOS TERMINOS ASENTADOS AL INICIO DE LA SESION.

SEGUNDO PUNTO LECTURA Y, EN SU CASO APROBACION DE LA ORDEN DEL DIA, YA SE DESAHOGO EN LOS TERMINOS ASENTADOS EN INICIO DE LA SESION.

TERCER PUNTO.- SE PROCEDE A LA PRESENTACION DEL MANUAL DE INTEGRACION Y FUNCIONAMIENTO DEL COMITÉ DE TECNOLOGIA DE INFORMACIÓN Y COMUNICACIONES DEL H. AYUNTAMIENTO DE ZIHUATANEJO DE

AZUETA, GUERRERO, LA CUAL SE CONFORMA DE SEIS TITULOS, CON SUS RESPECTIVOS CAPITULOS, MISMOS QUE SE ENCUENTRAN GLOSADOS EN EL PRESENTE MANUAL.
POR LO QUE EL PRESIDENTE PONE A CONSIDERACION DE LOS PRESENTES LA APROBACION DEL MANUAL DE INTEGRACION Y FUNCIONAMIENTO DEL COMITÉ DE TECNOLOGIA DE INFORMACIÓN Y COMUNICACIONES DEL H. AYUNTAMIENTO DE ZIHUATANEJO DE AZUETA, GUERRERO, POR LO QUE INSTRUYE AL SECRETARIO PARA QUE PROCEDA A SOLICITAR VOTACION CONFORME A LA LISTA DE ASISTENCIA, POR LO QUE EL SECRETARIO SOLICITA A LOS INTEGRANTES EMITAN SU VOTO PARA LA APROBACION O NO DEL MANUAL DE INTEGRACION Y FUNCIONAMIENTO DEL COMITÉ DE TECNOLOGIA DE INFORMACIÓN Y COMUNICACIONES DEL H. AYUNTAMIENTO DE ZIHUATANEJO DE AZUETA, GUERRERO, MEDIANTE VOTACION ECONOMICA, EL SECRETARIO DECLARA QUE SE APRUEBA POR UNANIMIDAD DE VOTOS EL MANUAL DE INTEGRACION Y FUNCIONAMIENTO DEL COMITÉ DE TECNOLOGIA DE INFORMACIÓN Y COMUNICACIONES DEL H. AYUNTAMIENTO DE ZIHUATANEJO DE AZUETA, GUERRERO,. EL PRESENTE MANUAL ENTRARA EN VIGOR EL DIA SIGUIENTE DE SU PUBLICACION DE LA GACETA MUNICIPAL DE ESTE MUNICIPIO DE ZIHUATANEJO DE AZUETA, Y SE DIFUNDIRA EN EL PERIODICO OFICIAL DEL ESTADO DE GUERRERO, ASI COMO EN LA PAGINA DE INTERNET OFICIAL PARA SU VALIDEZ RESPECTIVA.

CUARTO PUNTO.- SE PROCEDE A LA PRESENTACION DEL CALENDARIO DE LAS SESIONES ORDINARIAS PROGRAMADAS DEL COMITÉ DE TECNOLOGIA DE INFORMACIÓN Y COMUNICACIONES DEL H. AYUNTAMIENTO DE ZIHUATANEJO DE AZUETA, GUERRERO,. PARA EL AÑO FISCAL 2019.

POR LO QUE EL PRESIDENTE PONE A CONSIDERACION DE LOS PRESENTES LA APROBACION DEL CALENDARIO DE LAS SESIONES ORDINARIAS PROGRAMADAS DEL COMITÉ DE TECNOLOGIA DE INFORMACIÓN Y COMUNICACIONES DEL H. AYUNTAMIENTO DE ZIHUATANEJO DE AZUETA, GUERRERO PARA EL AÑO 2019, POR LO QUE INSTRUYE AL SECRETARIO PARA QUE PROCEDA A SOLICITAR VOTACION CONFORME A LA LISTA DE ASISTENCIA, POR LO QUE EL SECRETARIO SOLICITA A LOS INTEGRANTES EMITAN SU VOTO PARA LA APROBACION O NO DEL CALENDARIO DE LAS SESIONES ORDINARIAS PROGRAMADAS DEL COMITÉ DE TECNOLOGIA DE INFORMACIÓN Y COMUNICACIONES DEL H. AYUNTAMIENTO DE ZIHUATANEJO DE AZUETA, PARA EL AÑO FISCAL 2019, MEDIANTE VOTACION ECONOMICA, EL SECRETARIO DECLARA QUE SE APRUEBA POR UNANIMIDAD DE VOTOS EL CALENDARIO DE LAS SESIONES ORDINARIAS PROGRAMADAS POR EL COMITÉ TECNOLOGIA DE INFORMACIÓN Y COMUNICACIONES DEL H. AYUNTAMIENTO DE ZIHUATANEJO DE AZUETA, PARA EL AÑO FISCAL 2019.

QUINTO.- HABIÉNDOSE CUMPLIDO EL OBJETIVO DE LA PRESENTE, **EL LIC. JORGE SÁNCHEZ ALLEC**, DECLARA AGOTADO EL ORDEN DEL DIA, ASÍ COMO LA APROBACION DEL MANUAL DE TECNOLOGIA DE INFORMACIÓN Y COMUNICACIONES DEL H. AYUNTAMIENTO DE ZIHUATANEJO DE AZUETA, GUERRERO PARA EL AÑO 2019, ASI COMO APROBADAS LAS SESIONES ORDINARIAS QUE SE LLEVARAN A CABO EN EL AÑO FISCAL 2019, CON LO ANTERIOR SE DA POR TERMINADO EL PRESENTE ACTO A LAS **TRECE** HORAS**DEL DIA DE SU INICIO,** FIRMANDO PARA CONSTANCIA LOS QUE EN ELLA INTERVINIERON ----------

C. LIC. JORGE SÁNCHEZ ALLEC
PRESIDENTE MUNICIPAL

ING.ADALBERTO TOLEDO SALGADO
PRESIDENTE DEL COMITE

LIC. JUAN MANUEL JUAREZ MEZA
SECRETARIO TECNICO

LIC.MARIO MIRANDA FLORES
VOCAL

LIC. LISSETH DE JESÚS GUTIÉRREZ SOLÍS
VOCAL

LIC. ABEL ALCARAZ ALCANTAR
VOCAL

ING. ERICK JAVIER PINEDA SANCHEZ
VOCAL

LIC. SALVADOR MELESIO SANDOVAL
VOCAL

LIC. ERIKA VAZQUEZ GARCIA
ASESOR

LIC ELADIO MOSQUEDA GONZALEZ
ASESOR

REGLAMENTO DE LOS SISTEMAS DE INFORMACION DEL MUNICIPIO DE ZIHUATANEJO DE AZUETA

INDICE

TITULO PRIMERO

TITULO SEGUNDO
CONECTIVIDAD DE INTERNET.

TITULO TERCERO
ACCESO Y SEGURIDAD.

TITULO CUARTO
RED INALÁMBRICA Y MONITOREO.

El Ciudadano Lic. Jorge Sanchez Allec, Presidente Municipal Constitucional de Zihuatanejo de Azueta, Guerrero, representante del Ayuntamiento, Jefe de la Administración Municipal y encargado de ejecutar sus resoluciones y en uso de las facultades que le confieren al Municipio los Artículos 172 Fraccion I de la Constitución Política del Estado Libre y Soberano de Guerrero y 72 de la Ley Orgánica del Municipio Libre.

HACE SABER

Que el Honorable Ayuntamiento Constitucional de Zihuatanejo de Azueta, de conformidad con las bases normativas establecidas por el H. Congreso del Estado y en ejercicio de las facultades que le confieren los Artículos 115, Fracción II de la Constitución Política de los Estados Unidos Mexicanos, el Artículo 172 Fraccion I de la Constitución Política del Estado Libre y Soberano de Guerrero y 61 Fracción I y III de la Ley Orgánica del Municipio Libre.

CONSIDERANDO

En cumplimiento a lo dispuesto en el capítulo tercero del Bando de Policía y Gobierno para el Municipio de Zihuatanejo de Azueta, es necesario brindar seguridad a nuestros usuarios de equipos informáticos, por tal motivo, el ayuntamiento considera indispensable contar un orden normativo municipal que se adecué al contenido de las reformas constitucionales sobre seguridad informática.

Actualmente el H. Ayuntamiento Constitucional de Zihuatanejo de Azueta, cuenta con una intranet, misma que soporta la plataforma de la página web del municipio.

El derecho de acceso a la información favorece la transparencia en el gobierno y la rendición de cuentas de todos los servidores públicos.

Por su parte, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental obliga a todas las dependencias y entidades del gobierno federal a dar acceso a la información contenida en sus documentos, respecto, entre otras cosas, a su forma de trabajo, al uso de los recursos públicos, sus resultados y desempeño. Cualquier persona puede solicitar información a las instituciones públicas y obtenerla en forma rápida y sencilla, sin necesidad de identificarse, ni justificar el uso que dará a la misma. Además, esta Ley garantiza el derecho de las personas a la vida privada, al obligar a las instituciones a proteger los datos personales que tienen en sus archivos o bases de datos. De esta forma, distingue la información gubernamental, que es pública, de la información sobre las personas, que es confidencial. La Ley, aprobada en junio del año 2002 es producto de la participación de grupos de la sociedad que llevaron una iniciativa propia del Ejecutivo Federal al Congreso y los legisladores, quienes la aprobaron en forma unánime. Con base en la Ley, fue creado el Instituto Federal de Acceso a la Información Pública (ifai),un organismo autónomo encargado de garantizar a todas las personas el acceso a la información pública y la protección de sus datos personales que posee el gobierno federal.

Por lo anterior, es necesario de diseñar un nuevo reglamento en materia de Seguridad informática en el Municipio, partiendo de la base de esos nuevos ordenamientos legales de carácter estatal y federal, obedeciendo a que los requerimientos de la sociedad en esta materia; estableciendo los criterios que deberán observar los usuarios, para protección y uso racional de los sistemas informáticos, equipos de cómputo y de la información que en ellos se almacena.

Ello implica de manera indispensable e ineludible, el replanteamiento de nuevas y mejores políticas de usuarios, líneas de acción y estrategias para combatir de manera frontal a la inseguridad informática, la lentitud del internet, que tanto daño causa al Ayuntamiento de Zihuatanejo de Azueta.

Los aspectos innovadores que contemplan las leyes federales y estatales, incluyen las dependencias involucradas en los Sistemas. Se amplían las facultades y obligaciones que tienen los Ayuntamientos y quién los preside en materia de seguridad informática.

Por lo anterior, el H. Ayuntamiento Constitucional de Zihuatanejo de Azueta, ha tenido a bien expedir el siguiente:

REGLAMENTO DE LOS SISTEMAS DE INFORMACION DEL MUNICIPIO DE ZIHUATANEJO DE AZUETA.

TÍTULO PRIMERO

CAPÍTULO I DISPOSICIONES GENERALES.

ARTÍCULO 1.- Se entenderá por:

VIRUS INFORMÁTICO. Es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

TROYANO: Es un programa informático que tiene la capacidad de ocultarse dentro de otro de apariencia inofensiva, de tal forma que cuando este programa anfitrión es ejecutado el Troyano se carga en memoria y realiza la labor dañina para la que fue diseñado.

GUSANO: Es un programa que es capaz de duplicarse a sí mismo pero no es capaz de infectar a otros programas. Los Gusanos utilizan la red para copiarse a sí mismos y también puede duplicar distintas partes del disco duro.

DROPPER: Son programas diseñados específicamente para evitar su detección por parte de los antivirus. Su misión principal es la de transportar e instalar virus. Normalmente se cargan en memoria y esperan que ocurra un evento determinado para activar e infectar el sistema con el virus que contiene.

BOMBA: Programas cuya misión es activarse en un momento prefijado, normalmente utilizando para ellos el reloj del sistema aunque también puede responder al número de veces que se ejecuta un programa dado. Un ejemplo de actuación de este tipo de Bombas es la ejecución de una serie de órdenes indeseadas cuando el usuario teclea una secuencia dada de caracteres en el teclado.

MAIL BOMBER: Programas que pueden ser configurados para enviar grandes cantidades de correo a un mismo destinatario, saturando con ellos su buzón e incluso bloqueándolo. Muchas veces realizan este envío masivo a través de servidores de correos anónimos para evitar que sea detectado su origen.

HOAXES (Bromas): Mensajes de alarma que se envían por correo advirtiendo al personal de la existencia de determinados virus muy peligrosos (Generalmente desconocidos e inexistentes, noticias falsas, etc.) Su contenido es totalmente falso y su misión es provocar el pánico entre los internautas, consiguiendo que se produzca un envío masivo produciéndose una reacción en cadena a través de muchos destinatarios en la red.

JOKES: Una especie de broma de mal gusto que tienen por objeto hacer creer al usuario que ha sido contaminado por un virus, simulando el comportamiento que tendría un virus real pero sin dañar en lo más mínimo el sistema que lo acoge. Un Jokes podría mostrar en pantalla un mensaje de que ese disco duro se está formateando a la vez que aparece un barra de progreso que va avanzando.

ANTIVIRUS. Es un programa dedicado a detectar y eliminar virus.

SPAM: Correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

SPYWARE: Programa espía, es un software que recopila la información de otros ordenadores y la transmite a una identidad externa. Como consecuencias de una infección de spyware resulta:

Perdida de la privacidad.

Disminución del rendimiento del sistema.

Impedimento de navegación fluida por Internet.

Tipos de Spyware

- ADWARE: Son conocidos como pop-ups. El propósito de este programa espía es conseguir que se haga clic en los anuncios que aparecen.
- KEYLOGGERS: Es un programa que se instala en un equipo todo lo que el usuario escribe en el equipo. Puede ser especialmente peligroso porque los usuarios pueden escribir el nombre de usuario, contraseña e incluso información de tarjetas de crédito.
- PHISHING SCAMS: Se refiere al acto de introducir su información personal en un sitio web que usted cree que es confiable, pero en realidad no lo es. Los suplantadores de identidad crean páginas web que son casi idénticas a otros sitios web de instituciones bancarias a fin de obtener su usuario y contraseña. También es típico copiar sitios web de compras para obtener información de la tarjeta de crédito.
- BROWSER HIJACKING: Consiste en cambiar la página de inicio del navegador a una página con anuncios publicitarios. Es más molesto que peligroso.

ANTISPYWARE: Tipo de aplicación que se encarga de buscar, detectar y eliminar spywares o espías en el sistema.

CORTAFUEGOS: Un cortafuegos o firewall es un sistema que previene el uso y el acceso desautorizados a tu ordenador.

AUTENTICACION: Es el proceso mediante el cual un sistema informático verifica la identidad de una persona, de manera que permita el acceso si esta validación es positiva.

CONFIDENCIALIDAD: Es la propiedad de un documento o mensaje que únicamente está autorizado para ser leído o entendido por determinadas personas o entidades.

CONTRASEÑA: Es el mecanismo a través del cual se auténtica a un usuario, ya que esta es información secreta que sólo éste proporciona para controlar el acceso hacia algún recurso.

CUENTA: Es el nombre o instancia lógica a través del cual se identifica a usuario.

HARDWARE: Es la parte física de un equipo de cómputo y más ampliamente de cualquier dispositivo electrónico.

INSTITUCION: Se debe entender como referencia al H. Ayuntamiento.

RED INFORMATICA: El conjunto de equipos de cómputo interconectadas entre sí para compartir información.

SERVIDOR PUBLICO: Persona (trabajador) designada o nombrada para ocupar un puesto con plaza permanente o eventual en el H. Ayuntamiento.

SOFTWARE: Al equipamiento lógico o soporte lógico de una computadora, comprende el conjunto de los programas, sistema operativo y demás componentes lógicos necesarios para hacer posible la realización de una tarea específica.

USUARIO: Los servidores públicos de la Institución y terceros que se les asignan recursos informáticos, como herramienta de trabajo para el cumplimiento de sus funciones y actividades.

CAPÍTULO II
DE LAS REDES INTERNET E INTRANET.

ARTÍCULO 2. El Departamento de Tecnologías de la Información, Como área de apoyo de Oficialía Mayor, que en lo sucesivo se le abreviará (DTI), tiene encomendadas las funciones de diseñar e implementar los sistemas de cómputo, administrar los servicios y accesos a los sistemas de la red mundial Internet.

ARTÍCULO 3. El DTI, identificará los usos inadecuados e inseguros en los que el personal incurra en el manejo de los sistemas informáticos y equipos de cómputo, para evitar poner en riesgo la información que genera el H. Ayuntamiento Constitucional en sus procesos internos.

ARTÍCULO 4. El DTI, fomentará el uso racional y adecuado de los recursos informáticos del H. Ayuntamiento Constitucional, a través de la capacitación permanente, campañas de difusión y soporte técnico hacia el personal.

CAPÍTULO III
DEL USO ACEPTABLE DE LOS RECURSOS DE INFORMACIÓN

ARTÍCULO 5. Los usuarios que se les asignen equipos y/o sistemas informáticos propiedad de la Institución, serán responsables del manejo de la información en el desempeño de las actividades propias al cargo.

ARTICULO 6. El DTI es responsable de administrar, operar, asegurar y mejorar la infraestructura informática, con acciones que permitan otorgar los servicios informáticos necesarios para que el H. Ayuntamiento cumpla con sus funciones.

ARTÍCULO 7. El DTI es la única área responsable para administrar los equipos y sistemas informáticos del H. Ayuntamiento, por lo cual, los usuarios que

requieran alguna instalación, configuración o cualquier cambio de software o hardware deberá solicitarlo a dicha Unidad mediante oficio.

ARTÍCULO 8. El uso de dispositivos periféricos y de almacenamientos externos como: Memorias USB, Teléfonos Celulares, agendas electrónicas, etc, utilizados para la descarga, intercambio, traslado de información pública o privada se aplicaran las siguientes medidas:

I. Si el equipo es propiedad del Ayuntamiento deberá tener conocimiento el titular o el responsable del equipo, que se accederá a conectar el dispositivo externo.

II. Si el equipo es ajeno, antes de conectar deberá cerciorarse de que tenga instalado un antivirus y que éste se encuentre actualizado, para evitar poner en riesgo la información contenida en los periféricos.

III. Escanear el dispositivo con el programa antivirus, para detectar posibles infecciones.

ARTÍCULO 9. El usuario asume la responsabilidad en el proceso de intercambio de información utilizando los dispositivos periféricos y de almacenamiento.

TÍTULO SEGUNDO

CONECTIVIDAD DE INTERNET

CAPÍTULO I
SERVICIOS DE INTERNET

ARTÍCULO 10. Los usuarios podrán hacer uso de sus cuentas personales en los servicios de correo electrónico externos (Hotmail, Gmail, etc.) únicamente para propósitos personales y particulares, por lo que no podrán utilizarse este tipo de servicios para distribuir o almacenar información del H. Ayuntamiento, para tal fin se deberá solicitar un correo institucional en la página oficial a través del DTI, en el que deberá de enviar y recibir información.

ARTÍCULO 11. El DTI. Restringirá el servicio de mensajería instantánea local (MSN Messenger, Yahoo, Facebook, ICQ, entre otros), por lo que los servicios de mensajería instantánea, redes sociales, quedarán restringidos a menos que sean necesarios para funciones específicas del área de trabajo y sean aprobados por el director o responsable de la misma.

ARTÍCULO 12. El DTI. Como parte de las medidas de seguridad de la red informática, se proporcionará a los usuarios el acceso controlado a los servicios de Internet, que no representen riesgo a los equipos y sistemas informáticos, la productividad y/o disponibilidad de la red.

ARTÍCULO 13. El DTI. Habilitará los equipos necesarios por dirección para fines de comunicación institucional.

CAPÍTULO II
RESTRICCIONES SOBRE EL USO DE LOS EQUIPOS, REDES Y SISTEMAS.

ARTÍCULO 14. Queda estrictamente prohibido.

1. Copiar, mover, borrar o imprimir archivos electrónicos, donde no se hayan otorgado los permisos explícitamente a los usuarios.
2. Hacer uso indebido de los equipos de cómputo conectados a la red.
3. Transgredir cualquier recurso informático, sistemas o sitios de telecomunicaciones a los que no se esté permitido acceder.
4. Ejecutar herramientas de monitoreo de red que implique la intersección, manipulación o alteración de datos, así como monitoreo de puertos o de vulnerabilidades informáticas dentro y hacia fuera de las redes del H. Ayuntamiento, sin autorización de DTI.
5. Usar cualquier tipo de programa, comandos o enviar mensajes de cualquier tipo, con la intensión de interferir, deshabilitar los equipos de cómputo o comunicaciones, a través de cualquier vía, localmente o a través de la red.
6. El uso del correo electrónico y comunicaciones para:
    1. Distribuir "correos cadena" o cualquier forma de envío masivo de correos, ya que afecta el ancho de banda de la red. En caso de requerir el envío de información oficial a grupos de usuarios del H. Ayuntamiento, deberá realizarse a través de listas o grupos de distribución autorizados.
    2. Reenviar información de la cuenta de correo institucional a otra cuenta no institucional.

TÍTULO TERCERO
ACCESO Y SEGURIDAD.

CAPÍTULO I
USO DE LAS CUENTAS DE ACCESO Y CONTRASEÑAS

ARTÍCULO 15. Se proporcionarán a los usuarios cuentas de acceso a los recursos informáticos, las cuales serán personales e intransferibles y de uso institucional, protegidas a través de contraseñas. Estas contraseñas evitarán el acceso no autorizado a los recursos informáticos asignados a los usuarios, por lo que no deberán ser compartidas ni reveladas.

ARTÍCULO 16. Se podrá disponer de cuentas de correo institucional de la página por Dirección o Área Administrativa a fin de facilitar las actividades de su personal, siendo los titulares responsables del uso de dichas cuentas.

CAPÍTULO II CARACTERÍSTICAS DE LAS CONTRASEÑAS

ARTÍCULO 17. Las contraseñas contarán con una vigencia que determinará el titular del DTI, por lo que finalizado este periodo, el jefe del área notificará por escrito el cambio de usuario y contraseña para cada área respectiva.

ARTÍCULO 18. El DTI, establecerá el cumplimiento del uso de contraseñas robustas y del cambio periódico de la misma a través de la configuración de los equipos y sistemas informáticos.

ARTÍCULO 19. El Titular del área podrá solicitar DTI, el cambio de contraseña, mediante oficio, justificando la necesidad de la misma.

CAPÍTULO III
ACCESO REMOTO AUTORIZADO

ARTÍCULO 20. Los usuarios que por motivos de sus actividades institucionales requieran del acceso a los recursos informáticos del H. Ayuntamiento desde una conexión remota y externa con un equipo de cómputo permitido, deberán contar con la autorización del titular del área que opere los sistemas informáticos, solicitar y justificar ante el DTI, a fin de que sea configurado el acceso a través de un canal seguro.

CAPÍTULO IV
CONTROL DE ACCESO A LOS SISTEMAS INFORMATICOS

ARTÍCULO 21. El acceso a los sistemas informáticos se realizará a través de la definición de perfiles de usuario, obedeciendo el principio de acceso controlado con el menor privilegio, estableciendo la máxima protección.

CAPÍTULO V
ALTAS, BAJAS Y CAMBIOS EN ACCESOS AUTORIZADOS

ARTÍCULO 22. El titular de la Dirección o del área que tenga a cargo equipos informáticos, designará quien los opere y será el responsable de solicitar el acceso y el rol del usuario al DTI.

ARTÍCULO 23. DTI será la responsable de dar de alta a los usuarios con base en los permisos otorgados por el titular.

CAPÍTULO VI
SEGURIDAD DE LOS EQUIPOS DE COMPUTO PORTATIL (LAPTOP)

ARTÍCULO 24. Los equipos de cómputo portátil adquiridos con recursos del H. Ayuntamiento se conectarán a la red interna para el desempeño de las actividades propias del H. Ayuntamiento, por lo que se deberá establecer máxima protección. El cargo del usuario lo designara el área resguardante y lo solicitará mediante escrito, exponiendo las razones necesarias.

CAPÍTULO VII
CONFIGURACIÓN DE SEGURIDAD DE LOS EQUIPOS PORTATILES

ARTÍCULO 25. El DTI, es la única instancia autorizada para administrar los equipos de cómputo portátil del H. Ayuntamiento, por lo cual el usuario que requiera alguna instalación, configuración o cualquier cambio de software o hardware deberá solicitarlo a dicha Unidad.

TÍTULO CUARTO
RED INALAMBRICA Y MONITOREO.

CAPÍTULO I
USO DE LA RED INALAMBRICA

ARTÍCULO 26. La red inalámbrica ofrece un ancho de banda limitado, por lo que su uso es restringido y controlado. El usuario que requiera configurar el acceso de algún equipo de cómputo a dicha red, deberá solicitarlo al DTI.

ARTÍCULO 27. El uso de servicios de video y audio en demanda estarán limitados en esta red, por lo que de requerirlos, los usuarios deberán utilizar la red alámbrica.

ARTÍCULO 28. La red inalámbrica ofrecerá servicios exclusivamente al interior de las instalaciones del H. Ayuntamiento.

ARTÍCULO 29. No deberá compartirse la conectividad a la red inalámbrica con equipos no autorizados.

CAPÍTULO II MONITOREO DE RED INALÁMBRICA

ARTÍCULO 30. DTI monitoreará permanentemente la red inalámbrica, a fin de identificar riesgos de seguridad, violaciones, de ser necesario implementará acciones correctivas.

CAPÍTULO III
USO DE REDES EXTERNAS PARA LOS EQUIPOS PORTATILES.

ARTÍCULO 31. El usuario, en caso de encontrarse en instalaciones externas al H. Ayuntamiento deberá procurar utilizar redes públicas de proveedores con acceso autorizado y seguro, ya que de otra manera podría poner en riesgo la información institucional que se encuentre almacenada en el equipo portátil.

CAPÍTULO IV
MONITOREO DE LA SEGURIDAD INFORMATICA

ARTÍCULO 32. El DTI, mantendrá vigilancia permanente de la red de cómputo y los recursos informáticos del H. Ayuntamiento con la finalidad de identificar brechas de seguridad y evaluar el nivel de seguridad de la infraestructura informática de la Institución.

ARTÍCULO 33. El DTI, tendrá la facultad de ejecutar estos procesos de monitoreo de la seguridad informática.

ARTÍCULO 34. DTI, verificará periódicamente la red de cómputo, los equipos y sistemas informáticos. El área que pueda ser afectada temporalmente por estas revisiones en su funcionalidad o disponibilidad de los sistemas deberá ser notificada a través de un memorando interno.

TÍTULO QUINTO
POLITICAS DE SEGURIDAD DE INFORMACION DIGITAL.

CAPÍTULO I ATENCIÓN A INCIDENTES

ARTÍCULO 35. El DTI recurrirá a los procedimientos de atención a incidentes para revisar los equipos informáticos asignados a los usuarios, en caso de identificar algún incumplimiento de las políticas de seguridad informática, realizará las acciones correctivas.

CAPÍTULO II MEDIDAS DE PROTECCIÓN

ARTÍCULO 36. Los usuarios que hagan uso de los recursos informáticos deberán adoptar las siguientes medidas:

I. Evitar transmitir por medios electrónicos información de uso interno del H. Ayuntamiento a personas no relacionadas con la Institución.

II. Configurar protectores de pantalla en los equipos de cómputo de manera que se activen automáticamente después de 10 minutos de encontrarse desatendidos por parte de los usuarios.

III. Controlar el acceso y uso de la información mediante la asignación de permisos a los archivos electrónicos. Integrar una leyenda que permita a los usuarios dar el tratamiento adecuado en términos de la protección que requieran de la información contenida en los archivos.

CAPÍTULO III
INFORMACIÓN DE ACCESO RESTRINGIDO

ARTÍCULO 37. La información que sea clasificada como reservada o confidencial de conformidad con la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y el Acuerdo general que establece los órganos, criterios y procedimientos institucionales para la transparencia y acceso a la información pública del H. Ayuntamiento, deberá observar las medidas de protección antes señaladas.

CAPÍTULO IV RESPALDO DE INFORMACIÓN

ARTÍCULO 38. Será responsabilidad de los usuarios respaldar la información institucional crítica e importante, que tengan bajo su resguardo en los equipos de cómputo asignados, asegurando que estos respaldos se conserven íntegramente.

El DTI, proporcionará las herramientas tecnológicas para que los usuarios protejan y respalden la información antes señalada.

CAPÍTULO V
TRANSMISIÓN DE INFORMACIÓN POR CORREO ELECTRÓNICO.

ARTÍCULO 39. El usuario que envíe correos electrónicos institucionales, con información que sea exclusivamente de uso confidencial, deberá incluir la siguiente declaración, por lo que los involucrados en la comunicación deberán darle el tratamiento adecuado:

Declaración de confidencialidad:

I. Este mensaje contiene información de carácter confidencial, por lo que no debe ser alterado, reproducido o intercambiado con terceros ajenos a esta comunicación sin la autorización del emisor. La violación de esta confidencialidad será sancionada conforme a lo que marca la ley.

II. La información contenida en este mensaje sólo debe considerarse oficial y no repudiable para fines administrativos internos del H. Ayuntamiento si ésta se encuentra firmada digitalmente por el emisor.

CAPÍTULO VI
AMBITO DE APLICACION Y RESPONSABILIDAD

ARTÍCULO 40. Estas políticas son de cumplimiento obligatorio para todos los servidores públicos del H. Ayuntamiento, que hagan uso de la red de cómputo institucional, así como de los equipos y sistemas informáticos de la Institución. También son sujetos obligados los terceros que por motivos académicos, de proyectos, prestación o contrato de servicios profesionales hagan uso de los recursos informáticos del H. Ayuntamiento.

TITULO SEXTO
DEL SOPORTE TÉCNICO DE LOS EQUIPOS DE COMPUTO, DISPOSITIVOS E IMPRESORAS.

CAPÍTULO I
DEL SOPORTE TÉCNICO.

ARTÍCULO 41. EL DTI, tiene encomendadas las funciones de brindar soporte técnico a los equipos de cómputo, dispositivos e impresoras propias del H. Ayuntamiento Constitucional de Zihuatanejo de Azueta.

ARTÍCULO 42. El DTI, cuenta con personal profesional capacitado para brindar el soporte necesario a los equipos informáticos que presenten fallas en su funcionabilidad.

ARTÍCULO 43. El DTI, como parte del servicio eficiente y eficaz, mantiene el control en atención a los servicios, sabiendo de la urgencia y necesidad para el desempeño de sus funciones se sigue el siguiente proceso según se clasifique el caso:

I. **FALLA DEL SOFTWARE:** Se formatea el equipo de cómputo, se reinstala el software y se entrega funcionando el equipo.

II. **FALLAS DEL HARDWARE:** Se reemplaza la pieza en caso de existencia, de lo contrario se requisita al departamento de compras, si resulta muy costosa la pieza a reemplazar se da de baja el equipo y se requisita un equipo completo nuevo.

Ver anexos (anexo 1. Diagrama de flujo de atención a equipo informático)

ARTÍCULO 44. En los casos que se solicite equipo informático nuevo para las áreas del Ayuntamiento, el DTI recomendará el equipo necesario para satisfacer las necesidades para tal fin.

ARTÍCULO 45. El equipo de cómputo externo solo será atendido para mantenimiento preventivo y correctivo, por medio de oficio y lo deberá solicitar el titular del área, justificando la necesidad que el equipo opere en el departamento afín. El propietario del equipo asume la responsabilidad total del equipo y no podrá culpar al departamento por las fallas del Software o hardware que se le encuentren.

ARTÍCULO 46. Los usuarios que se les asignen equipos y sistemas informáticos propiedad de la Institución, serán responsables del buen uso en el desempeño de las actividades propias al cargo y solicitaran al DTI la limpieza del mismo.

ARTÍCULO 47. El uso de dispositivos periféricos y de almacenamientos externos como: Memorias USB, Teléfonos Celulares, agendas electrónicas se encuentra autorizado, siempre y cuando obedezca a las actividades legitimas profesionales del usuario.

ARTÍCULO 48. En caso de mantenimiento o reparación de los equipos, se dispondrá de los mecanismos necesarios para respaldar la información institucional que se encuentre en ellos almacenada, informan.

CAPÍTULO II

RESTRICCIONES SOBRE EL USO DE LOS EQUIPOS DE CÓMPUTO

ARTÍCULO 49. El DTI prohíbe las acciones siguientes:

1. Deshabilitar, desinstalar o modificar la operación del antivirus y herramientas de seguridad informática institucionales.
2. Distribuir programas maliciosos a través de la red informática, así como en documento adjunto de correos electrónicos (por ejemplo, virus informáticos, gusanos de internet, programas troyanos, entre otros).

3. Usar, descargar, almacenar o instalar cualquier herramienta para intercambio y descarga masiva de archivos como son las redes P2P (pear to pear) o similares (Ares, jdownloader, atubecatcher, etc.).
4. Transmitir material que se pueda considerar ofensivo.
5. Descargar, almacenar o reproducir en línea archivos de música, video, no relacionados con las actividades del H. Ayuntamiento.
6. No se puede extraer el equipo de cómputo de las oficinas
7. No podrán instalar y descargar software que no sea de ámbito laboral sin antes requerirlo mediante oficio correspondiente al jefe del área.

CAPÍTULO III

SEGURIDAD EN LOS EQUIPOS DE CÓMPUTO

ARTÍCULO 50. Las contraseñas generadas por los usuarios deberán:

I. Tener una longitud mínima de 8 caracteres.
II. Tener cuando menos un carácter mayúscula, uno minúscula y un carácter no alfabética (puede ser un número o un símbolo).
III. La contraseña no debe ser una palabra común o de diccionario, tampoco deberá estar basada en información personal, nombres de familiares, mascotas, etc.
IV. El titular del área será el responsable del uso de la contraseña y el compartir la misma con los de confianza.

TRANSITORIOS

Primero.- El presente Reglamento, entrará en vigor el día siguiente al de su Publicación en la Gaceta Municipal.

Segundo.- Se derogan todas las disposiciones que se opongan al presente Reglamento.

Tercero.- El Municipio celebrará Convenios de Coordinación con el Estado y la Federación con el objeto de ir implementando gradualmente la transparencia de la Información, protegiendo la información confidencial de la pública.

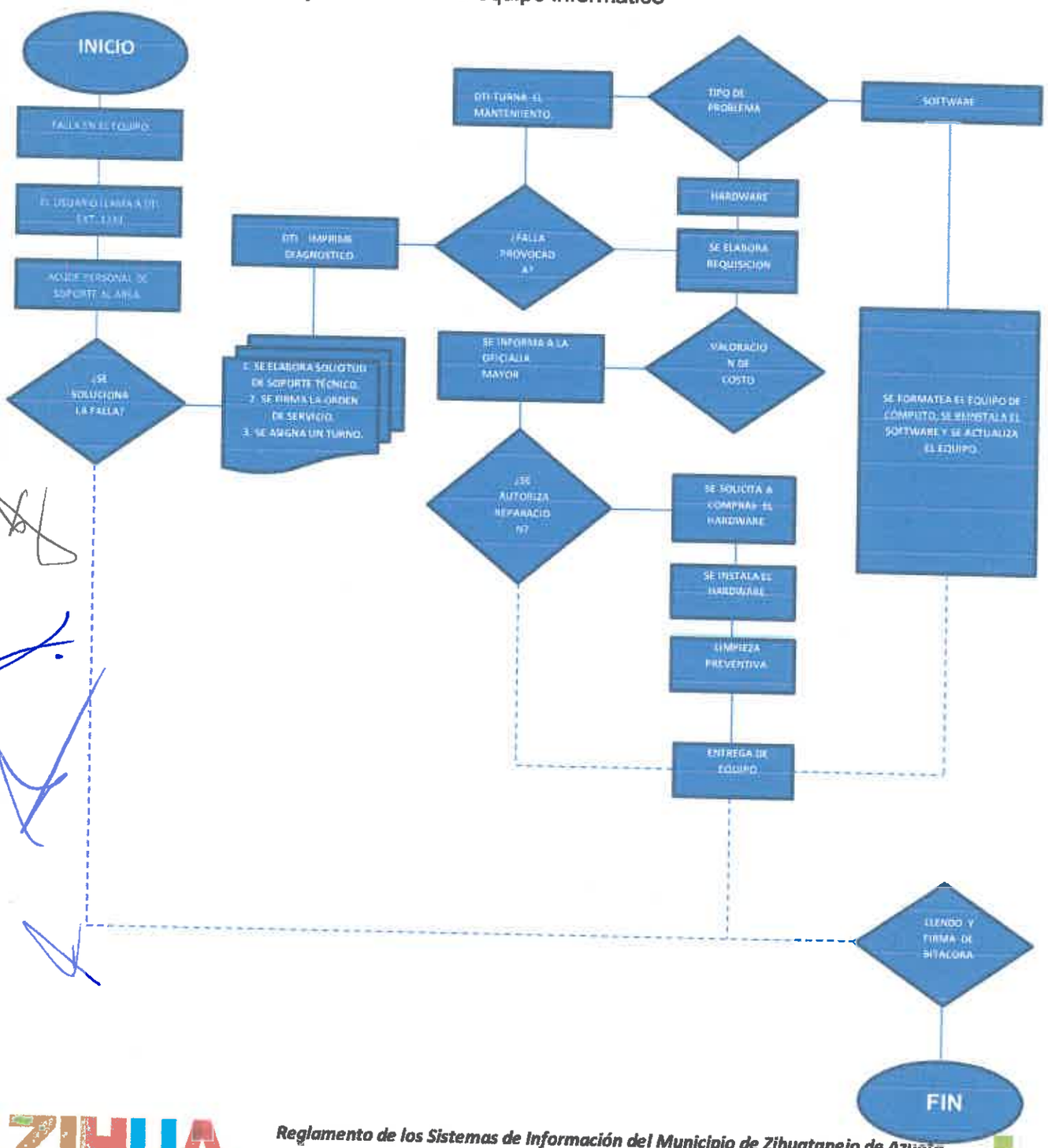
Quinto.- Cuando los privilegios de los Equipos, el manejo de información de alguna Regiduría, Dirección o Área, se cambie de adscripción, del personal, mobiliario, archivo y en general el equipo que aquélla haya utilizado, pasarán a la unidad que previamente se determine.

Sexto.- El comité de Tecnologias de la información se reunirá de manera bimestral para revisar los avances en la implemantación del manual.

ANEXOS

Anexo 1.

Diagrama de flujo de atención a equipo informático



Dado en la ciudad de Zihuatanejo en la sesion extraordinaria del H. Ayuntamiento de Zihuatanejo de Azueta, Estado de Guerrero a los 3 días del mes de Enero del 2019,

"SUFRAGIO EFECTIVO, NO RELELECCION"
H. AYUNTAMIENTO CONSITUCIONAL DEL MUNICIPIO DE ZIHUATANEJO DE AZUETA

PRESIDENTE MUNICIPAL
LIC. JORGE SANCHEZ ALLEC

SECRETARIO DEL AYUNTAMIENTO
LIC. JUAN MANUEL JUAREZ MEZA

SESION ORDINARIA DE COMITÉ DE TECNOLOGIAS DE LA INFORMACION 2019

NUMERO	MES	FECHA
1	ENERO - FEBRERO	2 ENERO DEL 2019
2	MARZO- ABRIL	3 MARZO DEL 2019
3	MAYO-JUNIO	5 MAYO DEL 2019
4	JULIO-AGOSTO	6 JULIO DEL 2019
5	SEPTIEMBRE-OCTUBRE	4 SEPTIEMBRE DEL 2019
6	NOVIEMBRE-DICIEMBRE	7 NOVIEMBRE DEL 2019