

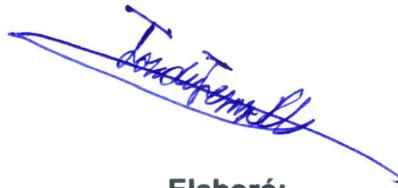


LINEAMIENTOS DE SEGURIDAD PARA LOS SISTEMAS INFORMÁTICOS.

**UNIDAD ADMINISTRATIVA: COORDINACIÓN DE SISTEMAS TIC'S
HUICHAPAN, HIDALGO AGOSTO 2022.**



PRESIDENCIA MUNICIPAL
HUICHAPAN - HIDALGO



Elaboró:

INFORMÁTICA Y SISTEMAS TIC'S Ing. José de Jesús Reyes López
Encargado del Departamento de Sistemas



Revisó:

L.A.E. Víctor A. Falcón López
Jefe de la Secretaría de Administración y Finanzas



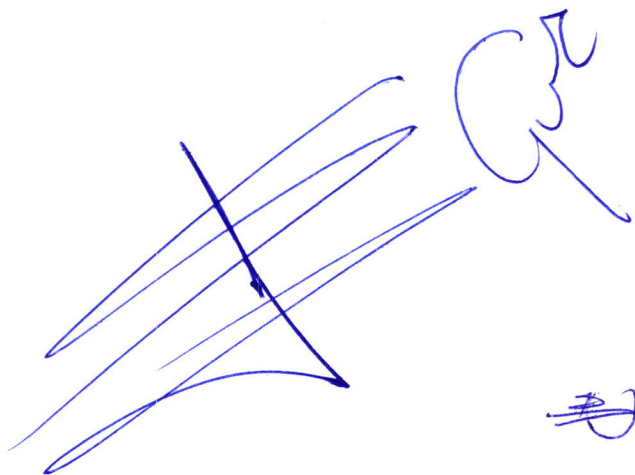
Aprobó:

C. Emeterio Moreno Magos
Presidente Municipal Constitucional de Huichapan

Fecha de emisión: AGOSTO 2022

Introducción	1
Marco Legal	2
Objetivo	2
Políticas informáticas que deberán de observar los usuarios	3
I. Sobre el uso de la tecnología de información y comunicaciones	3
II. Sobre el sortear y la seguridad lógica	4
III. Sobre el hardware y la seguridad física	5
IV. Sobre el uso de las impresoras	6
V. Sobre el respaldo, resguardo y restauración de información	7
VI. Sobre el correo electrónico institucional	8
VII. Sobre la publicación del contenido de la página web e intranet institucional	9
VIII. Sobre el uso de la firma electrónica avanzada FEA	9
IX. Sobre digitalización de la información	10
X. Sobre el equipo de cómputo propiedad del personal adscrito a la Administración Pública	10

Glosario



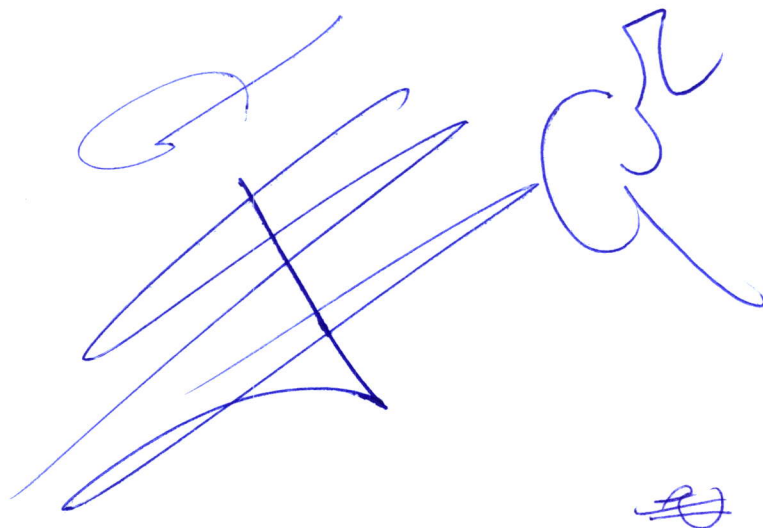
I. INTRODUCCIÓN.

La Tecnología de la Información y Comunicaciones es un elemento estratégico, que contribuye en la toma de decisiones y facilita el desarrollo de procesos y actividades de La Administración Pública.

La aplicación de las Políticas y Lineamientos para el uso y conservación de la Tecnología de la Información y Comunicaciones permite aprovechar al máximo los recursos para obtener resultados y mantener los estándares de eficiencia y eficacia que demandan las instituciones públicas.

Se requiere la responsabilidad de todos los trabajadores que integran La Administración Pública ya que la información que realizan y procesan en los equipos de cómputo se convierten en un archivo digital importante de La Administración Pública, por lo tanto, es prioritario que el personal este consciente que preservar la seguridad de la información es tarea de todos.

Es responsabilidad de todos los trabajadores que manejan archivos digitales y hacen uso de herramientas tecnológicas, conocer y dar cumplimiento a las Políticas y Lineamientos para el uso adecuado de las Tecnologías de la Información y Comunicaciones, ya que el incumplimiento a las mismas ocasionará daños en los procesos y actividades de La Administración Pública, por lo tanto se busca asegurar la integridad, disponibilidad, conservación y seguridad de la información, equipos de cómputo y equipos de almacenamiento de datos.

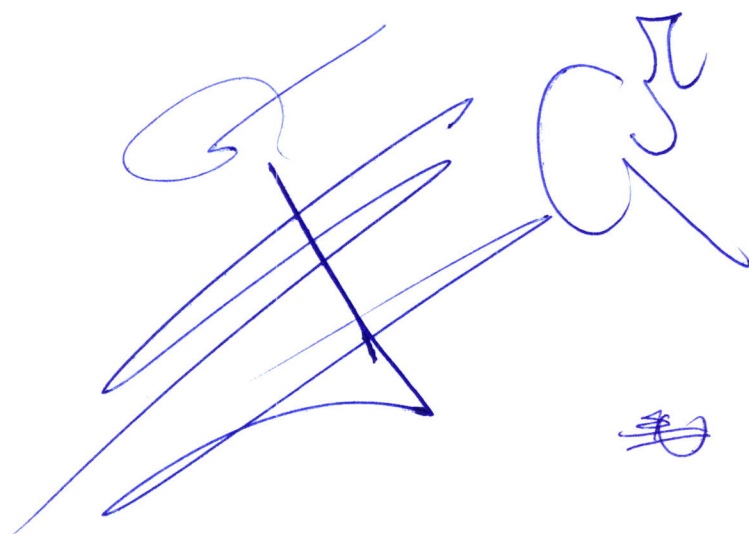


II. MARCO LEGAL

Con fundamento en los artículos 4 segundo párrafo y 74 fracción VIII de la Ley de Fiscalización Superior y Rendición de Cuentas del Estado de Hidalgo, publicada en el Periódico Oficial del Estado de Hidalgo de fecha 10 de julio del año 2017, y 10 fracción V del Reglamento Interior de la Auditoría Superior del Estado de Hidalgo, publicado el 12 de marzo de 2018 en la misma fuente de difusión oficial, y con el fin de mantener la confiabilidad, disponibilidad, accesibilidad e integridad de los activos digitales y recursos informáticos de la Auditoría Superior, el L.C.C. Armando Roldán Pimentel, Auditor Superior del Estado de Hidalgo emite las **“Políticas y Lineamientos para el Uso y Conservación de la Tecnología de Información y Comunicaciones”**. Y con fundamento en el Marco Estatal de Control Interno para el Sector Público del Estado de Hidalgo, título segundo, capítulo I, fracción 11.10, 11.11, 11.12 y 11.13.

III. OBJETIVO

Establecer lineamientos para el uso y conservación de las Tecnologías de la Información y Comunicaciones, con la finalidad de conservar la confiabilidad, accesibilidad e integridad de los archivos digitales y recursos informáticos de La Administración Pública.



POLÍTICAS INFORMÁTICAS QUE DEBERÁN DE OBSERVAR LOS USUARIOS

1.- SOBRE EL USO DE LA TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

1. El usuario será responsable de las cuentas y contraseñas que les son asignadas, por ninguna circunstancia, deberá proporcionar a terceros su cuenta y contraseña de acceso a la red institucional, sistemas, aplicaciones y/o aplicativos, salvo cuando se requiera para un proceso derivado de la baja del personal y que en su caso deberá de realizar la entrega a quien se le designe.
2. No deberá acceder a la información, sistemas o recursos que no correspondan a la naturaleza de sus funciones o a los que no esté autorizado, tampoco permitir o facilitar que otros lo hagan, con el fin de degradar la confiabilidad de la red institucional o que pongan en riesgo la continuidad del sistema informático, mediante software malicioso, robo de claves y de dirección del equipo en la red (IP).
3. Atenderá las medidas de seguridad y confidencialidad, que implemente la Dirección de Tecnología de la Información, sobre la producción, generación, emisión, publicación, intercambio, distribución y transmisión de datos e información.
4. Si durante la jornada laboral es necesario retirarse del área de trabajo deberá cerrar las aplicaciones, sistemas de información y en su caso, sesiones de Internet que esté ocupando; se recomienda bloquear el equipo presionando las teclas **Windows + L** para evitar que otra persona acceda a su información.
5. No deberá de alterar la configuración del software o hardware propiedad de La Administración Pública.
6. Deberá permitir que el personal de Sistemas acceda a la información contenida en los equipos de cómputo, con el fin de detectar, analizar y seguir los sucesos de una determinada sesión o conexión.
7. Quienes por la naturaleza de sus funciones laboran fuera de las instalaciones de La Administración Pública, no deberán guardar información propia de sus funciones en equipos de cómputo ajenos a los equipos institucionales, salvo casos específicos como equipos particulares debidamente registrados y autorizados.
8. Es responsabilidad de cada usuario el cuidado de las etiquetas de licencias de software de

los equipos de cómputo, si está adherida al equipo y en caso de que se desprenda, dar aviso inmediatamente al área de Sistemas.

9. Evitar saturar el espacio en disco duro con archivos multimedia (audio, video o imágenes) ajenos a sus actividades.

10. El compartir información con colaboradores de trabajo deberá realizarse sobre los canales oficiales de La Administración Pública (Correo Institucional, Sistema de Oficios, Tarjetas, OneDrive, Carpetas compartidas en servidores de datos)

2.- SOBRE EL SOFTWARE Y LA SEGURIDAD LÓGICA

1. El responsable y auxiliar de sistemas serán los únicos responsables de asignar las cuentas, claves de acceso, contraseñas, perfiles de usuarios de sistemas de información y bases de datos, al personal previamente autorizado, salvo que dentro del sistema o aplicativo las áreas tengan habilitada a una persona que cuente con la facultad de asignar o modificar perfiles.

2. Las cuentas de usuario asignadas son personales e intransferibles, por lo que el usuario será responsable de la información a la que tiene acceso y el uso de la misma.

3. Los usuarios serán responsables del software instalado en su equipo.

4. El área de Sistemas comunicará al usuario cuando el equipo de cómputo requiera cambio o instalación de software, licencias y/o programas.

5. Queda prohibido el uso de software o programas que no cuenten con licencia.

6. El secretario(a), director(a), subdirector(a), encargado(a) de departamento o coordinador(a) solicitará al área de Sistemas, para su consideración, el requerimiento de software de prueba (shareware) o de licenciamiento libre (freeware).

7. La instalación de software de uso libre o de prueba, previamente autorizado, será realizada sólo por el personal de Sistemas, de lo contrario cualquier consecuencia derivada de esta acción será responsabilidad del usuario.

8. Los usuarios serán responsables del software no autorizado que se encuentre instalado en su equipo.

9. No debe instalarse o utilizarse software de entretenimiento (por ejemplo: redes sociales, películas, juegos).

10. Los usuarios serán responsables de los datos con los que alimenten a los sistemas que utilizan para sus actividades laborales.

11. Será responsabilidad de cada secretario(a), director(a), subdirector(a), encargado(a) de departamento o coordinador(a), la notificación oficial mediante el Sistema de Oficios y Tarjetas Interinstitucionales al área de Sistemas, de cualquier movimiento de su personal que implique un cambio en el estatus y nivel de acceso de las cuentas de usuario que les hayan sido otorgadas.

12. Las cancelaciones de los siguientes servicios: acceso a la red institucional de datos, internet, correo institucional, acceso a sistemas y/o aplicativos, se realizarán conforme a lo siguiente:

- a) A petición del secretario(a), director(a), subdirector(a), encargado(a) de departamento o coordinador(a) en donde labora el usuario.
- b) Por hacer uso distinto al servicio asignado.

13. Es de suma importancia instalar todas las actualizaciones de software con el que cuente el equipo de cómputo, para evitar correr riesgos de seguridad, que comprometan la integridad de equipos y de la red de datos y comunicaciones.

3.-SOBRE EL HARDWARE Y LA SEGURIDAD FÍSICA

1. No exponer los equipos de cómputo a líquidos y alimentos.

- a) En caso de accidente:
 1. Apagar y desconectar inmediatamente el equipo del suministro de energía eléctrica.
 2. Si se trata de un equipo de cómputo laptop, de ser posible retirar inmediatamente la batería.
 3. Reportar al área de Sistemas.
 4. Reportar al Auxiliar de recursos materiales.

2. Se deberán desconectar los equipos de cómputo en los siguientes casos:

- a) De forma inmediata, cuando se produzca un corte de energía.
- b) Durante periodos vacacionales.
- c) Por cualquier otra causa imputable a fallas de energía eléctrica.

3. Al retirarse de la oficina no deberá dejar encendidos los equipos de cómputo, nobreaks o reguladores de voltaje.

4. En ninguna circunstancia intentará, por sí mismo, la reparación de cualquier equipo de

cómputo.

5. Para el préstamo de equipo de cómputo y comunicaciones, bajo resguardo del área de Sistemas, se deberá realizar solicitud por escrito mediante el Sistema de Oficios y Tarjetas Interinstitucionales.
6. Facilitar el equipo de cómputo a resguardo del usuario, al personal de Sistemas para que se realicen los programas de Mantenimiento Preventivo contenido en el Plan de Trabajo.
7. Será responsabilidad de cada secretario(a), director(a), subdirector(a), encargado(a) de departamento o coordinador(a), la notificación oficial al área de Sistemas, mediante el Sistema de Oficios y Tarjetas Interinstitucionales, de cualquier movimiento de su personal que implique una baja del equipo de cómputo, para mantener el control de la red y accesos a los sistemas informáticos de La Administración Pública.
8. El Auxiliar de recursos materiales será encargado de registrar los cambios al interior de las áreas de La Administración Pública, sobre el equipo de cómputo, derivados de los movimientos de personal asignado a dichas áreas, en el Sistema de Inventario.
9. En caso de cualquier daño físico a los equipos de cómputo que se deriven de un uso inadecuado por parte del usuario, se emitirá el reporte técnico para que el usuario acuda al área correspondiente a efecto de que se determine si el usuario realizará el pago de las reparaciones o en su caso la reposición del equipo.

4.- SOBRE EL USO DE LAS IMPRESORAS

1. Las impresoras son para uso exclusivo de documentación institucional, cualquier otro uso deberá ser autorizado por el jefe inmediato.
2. La impresión de material a color será restringida a documentos que por sus características ilustrativas así lo requieran.
3. Para la impresión de documentos se deben seguir las siguientes recomendaciones:
 - a) Si cuenta con la opción de imprimir en más de una impresora, seleccionar adecuadamente el equipo en el que va a imprimir.
 - b) Verificar que el tipo y tamaño de papel que esté en la impresora sea el adecuado.
 - c) Revisar la vista previa del documento que se va a imprimir para comprobar la presentación del mismo, antes de mandar la impresión.
 - d) Verificar y seleccionar las opciones de impresión como: Cantidad de impresiones, las hojas que desee enviar, tamaño del papel, el tipo de impresión que desee realizar, tipo de papel (normal, opalina, cartulina, etiquetas.)
 - e) Solo imprimir el documento cuando se esté seguro de que las opciones

seleccionadas sean las correctas.

f) Debe retirar inmediatamente los documentos impresos.

4. En caso de que el documento no se imprima, no volver a dar la instrucción de impresión y se recomienda, solicitar apoyo del personal de Sistemas.
5. Si la impresión tarda en salir, no oprimir ningún botón de la impresora, ya que esta puede perder la configuración o descomponerse; en tal caso, dar aviso al personal de Sistemas.
6. Evitar el uso de papel reciclado, ya que esto acelera el desgaste de las impresoras.
7. Evitar manipular con fuerza excesiva cualquier componente de las impresoras ya que esto puede provocar daños en la misma.
8. Cualquier daño físico a las impresoras es responsabilidad del área a cargo de esta.
9. El usuario no tiene permitido manipular el panel de control de las impresoras, ya que esto podría afectar la configuración de esta.

En caso de que en las diferentes áreas requieran de impresoras a resguardo del personal del área de Sistemas, se deberá realizar la solicitud mediante el Sistema de Oficios y Tarjetas Interinstitucionales.

5.- SOBRE EL RESPALDO, RESGUARDO Y RESTAURACIÓN DE INFORMACIÓN

1. Cada usuario es responsable de respaldar, o en su caso permitir que se elabore el respaldo de la información que produce y/o recibe para La Administración Pública, debiendo asegurarse de que esa información sea analizada previamente y se encuentre libre de virus.
2. Se sugiere que el respaldo de la información sea semanal, quincenal y como plazo máximo de forma mensual.
3. Se deben evitar nombres muy largos de archivos y carpetas, así como la ruta completa en la que se encuentran (el total para la ruta y nombre es de 256 caracteres) en caso contrario estos no podrían ser respaldados en forma masiva con el riesgo de perder la información.
4. Cuando el usuario observe problemas en el procedimiento de las copias de respaldo, el personal de Sistemas podrá colaborar realizando las acciones que favorezcan en mayor medida, a la seguridad de los datos.
5. Los respaldos consistirán, exclusivamente, de información de naturaleza laboral, omitiendo la personal o de otra índole (fotos, música, videos).

6. Los dispositivos externos como discos duros y memorias deben considerarse como medios de almacenamiento para respaldo, no como elemento de almacenamiento y de trabajo cotidiano, los archivos originales deberán permanecer en el equipo de cómputo que tiene a su resguardo.

7. Cuidar que los medios de almacenamiento no estén expuestos a condiciones o elementos (altas temperaturas, humedad, acumulación de polvo, etc.) que pudieran provocar daños.

6.- SOBRE EL CORREO ELECTRÓNICO INSTITUCIONAL

1. El secretario(a), director(a), subdirector(a), encargado(a) de departamento o coordinador(a) de La Administración Pública, solicitarán, mediante el Sistema de Oficios y Tarjetas Interinstitucionales, al área de Sistemas la asignación de cuentas de correo electrónico oficial para su personal, las cuales estarán sujetas para su autorización a la disponibilidad del servicio y deberán solicitar su cancelación cuando sea necesario.

2. El correo institucional es exclusivamente de uso oficial.

3. Es responsabilidad del usuario la cuenta y contraseña asignada, debido a que es personal e intransferible.

4. Por seguridad, no abrir ningún mensaje o archivo adjunto de remitentes desconocidos.

5. Siempre se deben tomar las precauciones correspondientes respecto a los archivos adjuntos como son:

- a) Nunca abrir o ejecutar directamente archivos adjuntos.
- b) Debe guardar primero en una carpeta temporal o en el escritorio.
- c) Revisar descargados con el antivirus institucional actualizado.
- d) Ante cualquier duda, deberá borrar el mensaje y los archivos adjuntos.

6. No abrir e inmediatamente eliminar los mensajes que contengan las siguientes características:

- a) Alertas sobre virus
- b) SPAM (mensajes de temática religiosa, leyendas urbanas, métodos para hacerse millonario, regalos de grandes compañías, etc).
- c) Malware

Nota: Actualmente existen numerosas amenazas que ponen en riesgo el equipo y la información como: Malware, Phishing, Ransomware, Stalkerware, y en muchos casos se propagan mediante correo electrónico, si tienes dudas al respecto dirígete al área de

Sistemas.

7.- SOBRE LA PUBLICACIÓN DEL CONTENIDO DE LA PÁGINA WEB E INTRANET INSTITUCIONAL

1. El secretario(a), director(a), subdirector(a), encargado(a) de departamento o coordinador(a) de La Administración Pública, solicitarán mediante el Sistema de Oficios y Tarjetas Interinstitucionales al área de Sistemas la publicación o creación de nuevas secciones dentro de los portales correspondientes de esta Institución especificando:

- a) Sección o apartado donde estará la publicación dentro del portal web o intranet.
- b) El archivo será entregado en el formato deseado o necesario con la solicitud de publicación previamente autorizada.
- c) Especificar los títulos que llevará la publicación.

2. Dependiendo de la complejidad de la información y la adecuación de la misma dentro del portal web, será el tiempo de publicación, por lo que se les pide tomar sus precauciones al entregar la información para dicha publicación. El horario de recepción de información será de 8:30 a 15:00 hrs.

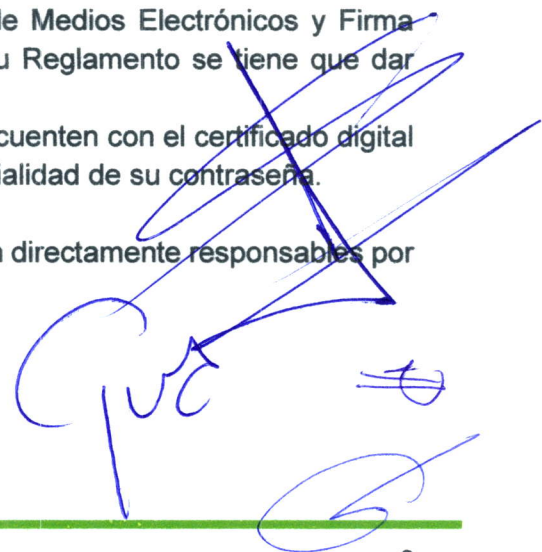
3. En el contenido del portal Web Institucional existe información que es alimentada por los diferentes sistemas que se tienen dentro del Organismo, la información de estos sistemas es responsabilidad de las diferentes Unidades, por ejemplo:

- a) Catálogo de Entidades Fiscalizadas.
- b) Directorio de servidores públicos.
- c) Reporte de Entrega de información trimestral.
- d) Reporte de Entrega en tiempo del Informe Anual de la Cuenta Pública.

8.- SOBRE EL USO DE LA FIRMA ELECTRÓNICA AVANZADA (FEA):

Con fundamento en lo dispuesto en la Ley Sobre el Uso de Medios Electrónicos y Firma Electrónica Avanzada (FEA) para el Estado de Hidalgo y su Reglamento se tiene que dar cumplimiento a lo siguiente:

1. Los servidores públicos de La Administración Pública que cuenten con el certificado digital de datos para el uso de la FEA deberán guardar la confidencialidad de su contraseña.
2. Los servidores públicos de La Administración Pública serán directamente responsables por los documentos firmados mediante el uso de la FEA.
3. Deberán mantener vigente su certificado digital.



4. En caso de olvidar la contraseña o extraviar el certificado digital, cambio de cargo o puesto de área de adscripción, deberán realizar el trámite correspondiente y contactar con quien realizaron su trámite de certificación digital.

- a) Entidad Certificadora del Gobierno del Estado de Hidalgo.
- b) Enlace de Certificación Digital de la ASEH.

9.- SOBRE DIGITALIZACIÓN DE LA INFORMACIÓN

1. Privilegiar el uso de archivos digitales.
2. Evitar la impresión de documentos (Informes, oficios, tarjetas informativas) que pueden ser consultados de forma digital.
3. Uso obligatorio del correo institucional, para la comunicación interna de La Administración Pública.
4. Uso de la Firma Electrónica Avanzada, para dar validez a:
 - a) Las acciones de fiscalización.
 - b) Comunicación entre las Entidades Fiscalizadas y La Administración Pública.
 - c) Comunicación entre las Unidades Administrativas de La Administración Pública.
5. Evitar la saturación en los equipos de cómputo de trabajo con el uso del almacenamiento externo asignado a esa actividad.
6. La solicitud de carpetas de uso compartido en los servidores de datos de La Administración Pública será por medio de oficio o tarjeta, firmada por el subdirector(a), encargado(a) de departamento o coordinador(a).
7. Clasificar el almacenamiento de la información por años para depurar los archivos digitales, según las fechas de conservación de información, que indique la normativa vigente.

10.- SOBRE EL EQUIPO DE CÓMPUTO PROPIEDAD DEL PERSONAL ADSCRITO A LA ADMINISTRACIÓN PÚBLICA.

1. Si el personal de La Administración Pública ingresa equipo de cómputo de su propiedad para ser utilizado como herramienta de trabajo y requiere acceso a conexión de internet deberá cumplir con el siguiente procedimiento:
 - a) El subdirector(a), encargado(a) de departamento o coordinador(a) que corresponda, deberá remitir mediante el Sistema de Oficios y Tarjetas Interinstitucionales al área de Sistemas, la solicitud para que el equipo se ingrese a la red de internet. La cual deberá contener lo siguiente:
 1. Nombre del usuario
 2. La marca, modelo y número de serie del equipo de cómputo
 3. Indicar los servicios que requiere cada equipo, ejemplo:
Impresoras.

Carpetas de archivos compartidos, en los servidores de datos.

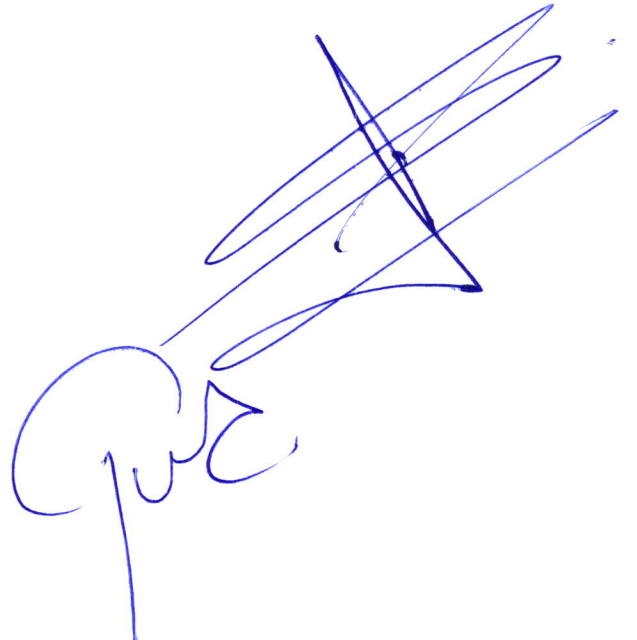
Acceso a sistemas institucionales.

Periodo en el cual se utilizará el equipo o bien, informar al área de Sistemas cuando se deban cancelar los accesos.

b) El equipo de cómputo será previamente valorado por el personal de Sistemas, para verificar si cumple con los requerimientos de hardware y software para ser ingresado a la red de datos y se analizará para detectar cualquier amenaza de virus.

c) El equipo de cómputo deberá contar con un software antivirus aprobado por el área de Sistemas, en caso contrario el acceso a internet será denegado.

2. El área de Sistemas elaborará su registro técnico y llevará el control de acceso a la red de internet.



GLOSARIO

- **La Administración Pública:** órgano del Municipio de Huichapan, Hidalgo del sector público conformados para realizar la tarea de administrar y gestionar organismos, instituciones y entes del Estado.
- **Activos digitales:** Los activos digitales a diferencia de los físicos, no se agotan con su consumo. Las empresas que crean valor con activos digitales podrán recolectar a través de un numero potencialmente infinito de transacciones esto incluye documentos, correos electrónicos, fotografías, MP3, películas online, y cualquier otro contenido que almacenar en un ordenador. (Tecnologías de Información, Gestión de Activos Digitales, 2016) (Tapscott, s.f.)
- **Configuración:** Es un conjunto de datos que determina el valor de algunas variables de un programa o de un sistema Operativo. Adaptar una aplicación software o un elemento hardware al resto de los elementos del entorno y a las necesidades específicas del usuario. Es una tarea esencial antes de trabajar con cualquier nuevo elemento. (Master Magazine, s.f.)
- **Dirección IP:** Las direcciones IP (Internet Protocol, Protocolo de Internet) son un número único e irrepetible que identifica una interfaz como única. La interfaz es un dispositivo como la tarjeta de red, punto de acceso. (Niño, s.f.)
- **Hardware:** Denominamos Hardware a la parte física del sistema, es decir el conjunto de dispositivos, cables, transistores, etc. que lo conforman. (Carrillo, s.f.)
- **Intranet Institucional:** Red informática que utiliza la tecnología del protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización. Puede estar formada por más de una red sin embargo son de acceso privado para los usuarios de la empresa. (Leon, s.f.)
- **Licencia:** Es un instrumento legal donde el desarrollador permite que su software sea distribuido y/o modificado. (Algesa.com.ar, s.f.)
- **Programas Freeware:** Los autores los ponen a disposición gratuitamente y se pueden usar, copiar, difundir, etc., gratuitamente, pero no pueden modificarse sin el consentimiento del autor. (DABURON B. E., s.f.)
- **Red institucional (corporativa):** La red de área local nos va a permitir compartir bases de datos, programas y periféricos como puede ser un módem, una impresora, un escáner, entre otros; poniendo a nuestra disposición otros medios de comunicación como pueden ser el correo electrónico y el chat. Además una red de área local sobrelleva un importante ahorro, tanto de dinero, ya que no es preciso comprar muchos periféricos, se consume menos papel, y en una conexión a Internet se puede utilizar una única conexión telefónica compartida por varios ordenadores conectados en red; como de tiempo, ya que se logra gestión de la información y del trabajo. (monografias.com, s.f.)
- **Shareware:** Se pueden obtener por descarga o por copia gratuita y después utilizar de forma gratuita durante un periodo de tiempo llamado periodo de prueba; a partir de ese momento, se supone que el usuario debe enviar una cantidad de dinero a cambio de una licencia de utilización oficial. (DABURON B. E., s.f.)
- **Software:** Todos aquellos conceptos, actividades y procedimientos que dan como resultado la generación de programas para un sistema de computación. (Ramírez, s.f.)
- **Software malicioso:** Tipo de software cuyo objetivo es provocar daños en un sistema informático, pueden ser virus, gusanos informáticos, troyanos. (MARIA DEL PILAR ALEGRE RAMOS, s.f.)
- **FEA:** Firma Electrónica Avanzada.

BIBLIOGRAFÍA

Algesa.com.ar. (s.f.). Obtenido de http://www.algesa.com.ar/Dic/licencia_de_software.php

Carrillo, A. G. (s.f.). books.google. Obtenido de:

<https://books.google.com.mx/books?id=OC17arE5xuC&pg=PA2&dq=definicion+hardware&hl=es&sa=X&ved=0ahUKEwiWrdmF1PTSAhUFMSYKHdJLAQAQ6AEIGjAA#v=onepage&q=hardware&f=false>

DABURON, B. (s.f.). DABURON, B. E. (s.f.). book.google. Obtenido de:

<https://books.google.com.mx/books?id=rO3Ed0DSGG8C&pg=PA110&dq=que+es+freeware&hl=es&sa=X&ved=0ahUKEwiqg6yv2vXSAhXPZiYKHZUtCNSQ6AEIRDAI#v=onepage&q=que%20es%20freeware&f=false>

Gómez, J. A. (s.f.). books. google. Obtenido de:

<https://books.google.com.mx/books?id=vhit3ZmGQPsC&pg=PA220&lpg=PA220&dq=Es+el+intermediario+de+la+comunicaci%C3%B3n+en+una+red+inal%C3%A1mbrica+con+topolog%C3%ADa+en+modo+infraestructura,+que+se+comunica+por+ondas+de+radio,+es+decir,+que+act%C3%BAa+de+pue>

León, C. Y. (s.f.). books.google. Obtenido de:

<https://books.google.com.mx/books?id=vbXYgr3AdAkC&pg=PA341&dq=intranet+definicion&hl=es&sa=X&ved=0ahUKEwiq5f43 TSAhWDQIYKHAFrBNYQ6AEIHAB#v=onepage&q=intranet%20definicion&f=false>

MARIA DEL PILAR ALEGRE RAMOS, A. G.-C. (s.f.). book.google. Obtenido de:

<https://books.google.com.mx/books?id=c8kni5g2Yv8C&pg=PA70&dq=Software+malicioso&hl=es&sa=X&ved=0ahUKEwiSmtSq7vXSAhXGbiYKHxWqA64Q6AEIITAB#v=onepage&q=Software%20malicioso&f=false>

Master Magazine. (s.f.). Obtenido de <https://www.mastermagazine.info/termino/4404.php>

monografias.com. (s.f.). Obtenido de <http://www.monografias.com/trabajos96/red-area-local/red-area-local.shtml>

Niño, J. (s.f.). books.google. Obtenido de:

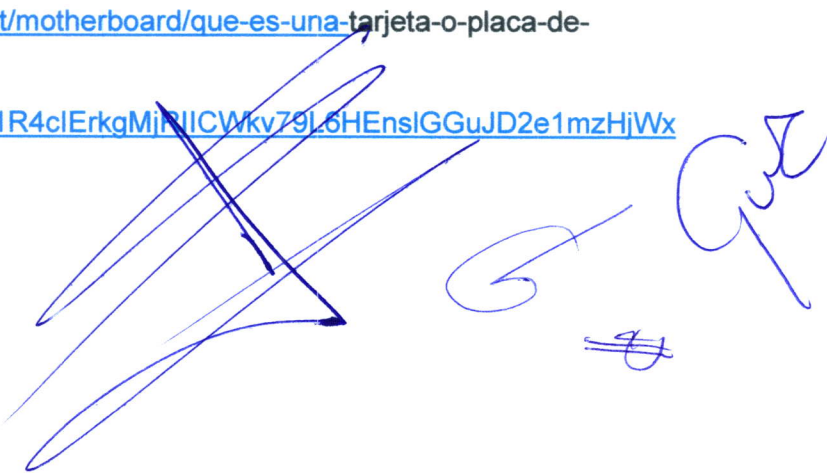
https://books.google.com.mx/books?id=6QXTAAwAAQBAJ&pg=PA283&dq=direccion+ip&hl=es&sa=X&redir_esc=y#v=onepage&q=direccion%20ip&f=false

Partes de una computadora. (s.f.). Obtenido de:

<http://www.partesdeunacomputadora.net/motherboard/que-es-una-tarjeta-o-placa-de-red/tarjeta-de-red-usb-externa>

RAMIREZ, B. S. (s.f.). Obtenido de:

https://docs.google.com/presentation/d/1R4clErkgMjNlICWkv79L6HEnsIGGuJD2e1mzHjWxSRY/edit#slide=id.g11b0c7260_05



Firma Integrantes del Comité de Control Interno y Desempeño del Municipio de Huichapan, Hidalgo.



Primera Sesión Ordinaria Ejercicio 2022
Agosto 2022

C. Emeterio Moreno Magos
Presidente Municipal Constitucional de Huichapan
y Presidente del Comité de Control Interno y
Desempeño del Municipio de Huichapan, Hidalgo.



CONTRALORÍA

Mr. General Municipal López
Titular del Órgano Interno de Control y Vocal
Ejecutivo del Comité de Control Interno y
Desempeño del Municipio de Huichapan,
Hidalgo.

Ing. Citlali Olivia Rodríguez Siordia
Síndico Procuradora y Vocal Ejecutivo del
Comité de Control Interno y Desempeño del
Municipio de Huichapan, Hidalgo.



L.D. Alejandra Esmeralda Pérez Carrillo
Secretaría General y Vocal del Comité de
Control Interno y Desempeño del Municipio de
Huichapan, Hidalgo.



A.A.E. Víctor A. Falcón López
Secretario de Administración y Finanzas y Vocal
del Comité de Control Interno y Desempeño del
Municipio de Huichapan, Hidalgo.



UNIDAD DE PLANEACIÓN
C.P. y A.P. Martha Lugo Jaramillo
Encargada de la Unidad de Planeación y Evaluación
y Vocal del Comité de Control Interno y Desempeño
del Municipio de Huichapan, Hidalgo.