



Instituto de Transparencia, Acceso a la Información Pública Gubernamental  
y Protección de Datos Personales del Estado de Hidalgo

Pachuca de Soto, Hgo., a 26 de noviembre de 2019.

No. de Oficio. ITAIH/DTI/076/2019.


**L.A. ELIA TEJEDA SALINAS**  
**TITULAR DE ÓRGANO INTERNO DE CONTROL**  
**DEL ITAIH**  
**P R E S E N T E**

Por medio del presente me permito enviarle los Lineamientos para la Recuperación de Desastres y Lineamientos para la Seguridad Informática, con el objetivo de que puedan ser integrados en el Modelo de Marco Integrado de Control Interno de este Instituto.

Sin más por momento quedo pendiente para cualquier duda o comentario al respecto.

ATENTAMENTE

  
**I.S.C. LEVY JOVANNY AMBROSIO JUARICO**  
**DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN**

	INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE HIDALGO
	26/11/19 <span style="float: right;">13:22</span> RECIBIDO ÓRGANO INTERNO DE CONTROL

RECIBI DOCUMENTOS



**Instituto de Transparencia, Acceso a la Información  
Pública Gubernamental y Protección de Datos  
Personales del Estado de Hidalgo**

**Dirección de Tecnologías de la  
Información**

**LINEAMIENTOS PARA LA RECUPERACIÓN DE  
DESASTRES DEL ITAIH**

# ÍNDICE

<b>Introducción</b>		<b>3</b>
<b>Normatividad aplicable</b>		<b>3</b>
<b>Lineamientos</b>		<b>4</b>
<b>Capítulo 1</b>	De los equipos de computo	<b>5</b>
<b>Capítulo 2</b>	De los equipos de telecomunicaciones	<b>6</b>
<b>Capítulo 3</b>	De los equipos de soporte eléctrico	<b>6</b>
<b>Capítulo 4</b>	De los servidores de datos	<b>7</b>

## **INTRODUCCIÓN**

El presente documento tiene la finalidad de servir como una guía para la recuperación de desastres en el supuesto de que se llegara a presentar un fallo dentro de la infraestructura tecnológica del ITAIH.

Esto con el objetivo principal de poder brindar un soporte técnico adecuado, asegurando la continuidad de los servicios a todas las áreas que integran el ITAIH y a su vez preservando que el ciudadano pueda ejercer su derecho de acceso a la información y la protección de datos personales en posesión de los sujetos obligados del Estado de Hidalgo.

## **NORMATIVIDAD APLICABLE.**

Los ordenamientos jurídicos administrativos vigentes que regulan la operación de las actividades o tareas específicas a normar a través de los lineamientos para la recuperación de desastres, entre otros son:

- Constitución Política para el Estado de Hidalgo.
- Ley de Transparencia y Acceso a la Información Pública para el Estado de Hidalgo.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo.

## **LINEAMIENTOS.**

Los términos y definiciones utilizados en el presente documento son:

**ITAIH:** Instituto de Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales del Estado de Hidalgo.

**DTI:** Dirección de Tecnologías de la Información.

**Usuario:** Todo empleado o funcionarios de los sujetos obligados del Estado de Hidalgo que hagan uso de los activos o servicios informáticos de la institución, para el desempeño de sus funciones, consulta o atención al servicio.

**Activo informático:** Son recursos de sistemas informáticos o relacionados con este, que son necesarios para el desempeño de las funciones del usuario, tales como equipos de cómputo, impresoras, video proyectores, teléfonos, equipos de telecomunicaciones, software, información, entre otros.

**Equipo móvil:** Es todo activo informático físico que tiene la facilidad de movilidad, como laptops, tabletas, teléfonos inteligentes, entre otros.

**Servicio informático:** Bien intangible que se proporciona para satisfacer los requerimientos de los usuarios, relacionado con el uso de activo informático.

**Medio de almacenamiento removible:** Medio externo al equipo de cómputo en el que se almacena información, como disquetes, CD, DVD, memorias (USB, SD, otras), discos externos y otros.

**Base de datos:** Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

**Software institucional:** Software con licenciamiento de uso y/o propietario que puede ser instalado y utilizado por los usuarios para el desempeño de sus actividades o funciones, o para la gestión de un servicio informático otorgado por la institución.

**Software libre:** También conocido como freeware, shareware, software demo. Software gratuito proveniente de internet o cualquier otro medio que no requiere la compra de una licencia para su uso.

**Web, www (World Wide Web):** Es una convergencia de conceptos computacionales para presentar y enlazar información que se encuentra dispersa a través de Internet en una forma fácilmente accesible.

**Virus:** Programa informático creado para producir daño en el equipo informático.

### **Capítulo 1. De los equipos de cómputo.**

- A. Para salvaguardar la información contenida en todos los equipos de cómputo del ITAIH, personal de la Dirección de Tecnologías de la Información realiza respaldos de manera bimestral, en base a un cronograma de trabajo establecido.
- B. Adicional es responsabilidad del usuario realizar respaldos de la información que genera con la periodicidad que crea pertinente, esto con el objetivo de siempre tener resguardada su información.
- C. En el caso que algún equipo de cómputo propiedad del ITAIH sufra daño físico en el disco duro, personal de la Dirección de Tecnologías de la Información evaluará el tipo de afectación presentada. Si es moderado se procederá a extraer la información por medio de software especializado en la recuperación de la información.

En el caso que sea un daño grave y la información a recuperar se considere de importancia alta, el disco duro se enviara a un centro especializado en la recuperación de información.

- D. Si el daño presentado se considera de hardware, se procederá a reemplazar la pieza afectada a la brevedad posible. Si el fallo es catalogado de software, se comenzará a realizar las configuraciones pertinentes para corregir la problemática de manera inmediata.

## **Capítulo 2. De los equipos de telecomunicaciones.**

- A. Si llegara a fallar algún firewall de seguridad, se cuenta con dos adicionales que servirán para corregir la problemática, mientras tanto el equipo dañado se manda a garantía para su reparación o en su defecto se reemplazara en su totalidad.
- B. Si llegara a fallar algún switch de red, se cuenta con dos adicionales que servirán para corregir la problemática, mientras tanto los dañados se mandan a garantía o se reemplaza en su totalidad.
- C. En el caso de presentar alguna falla el enlace dedicado del servicio de internet, contamos con 5 servicios adicionales de internet de alta velocidad para corregir la falla presentada y seguir con la operación de los diferentes sistemas informáticos con los que cuenta el ITAIH.

## **Capítulo 3. De los equipos de soporte eléctrico.**

- A. Cada equipo de cómputo que forma parte de la infraestructura tecnología del ITAIH, cuenta con regulador y respaldo de voltaje (No-break), con la finalidad de proteger su operación por cualquier corte de energía o sobrecarga eléctrica. De presentarse fallas de funcionamiento en alguno de los No-break, estos se reemplazarán a la brevedad posible.
- B. Respecto a los servidores de aplicaciones, contamos con equipos de alimentación ininterrumpidas (UPS) dedicados a proporcionar el voltaje adecuado por cualquier corte de energía o sobrecarga eléctrica, logrando mantener siempre en activo los servidores mencionados. De presentarse fallas de funcionamiento en alguno de los UPS, se reemplazarían a la brevedad posible.
- C. Se cuenta con planta de luz, que es la encargada de proporcionar energía cuando existe algún corte del suministro eléctrico, de esta manera se asegura siempre que el SITE del ITAIH opere de manera adecuada y continua.

#### **Capítulo 4. De los servidores de datos.**

- A. Contamos con 4 servidores encargados de hospedar los diversos sistemas institucionales con los que cuenta el ITAIH. Dos son catalogados como productivos, es decir son los que están brindando servicio las 24 horas y dos catalogados como espejo, que su función es mantener respaldos de los servidores productivos.
  
- B. Si algún servidor catalogado como productivo llegara a presentar algún fallo, de manera inmediata se pone en funcionamiento alguno de los servidores catalogados como espejo, asegurando de esta manera el continuo servicio de los servidores mencionados.
  
- C. Si el fallo que llegara a presentar alguno de los servidores mencionados es catalogado de hardware, se procedería a reemplazar la pieza afectada de manera inmediata. Si el fallo es catalogado de software, se comenzará a realizar las configuraciones pertinentes para corregir la problemática de manera inmediata.





**Instituto de Transparencia, Acceso a la Información  
Pública Gubernamental y Protección de Datos  
Personales del Estado de Hidalgo**

**Dirección de Tecnologías de la  
Información**

**LINEAMIENTOS PARA LA SEGURIDAD  
INFORMÁTICA DEL ITAIH**

# ÍNDICE

<b>Introducción</b>		<b>3</b>
<b>Alcance</b>		<b>3</b>
<b>Normatividad aplicable</b>		<b>3</b>
<b>Lineamientos</b>		<b>4</b>
<b>Capítulo 1</b>	De la seguridad informática en la institución	<b>4</b>
<b>Capítulo 2</b>	Del buen uso de los activos informáticos	<b>6</b>
<b>Capítulo 3</b>	De la clasificación de la información	<b>6</b>
<b>Capítulo 4</b>	Del intercambio de información	<b>7</b>
<b>Capítulo 5</b>	De la prestación de servicios por terceros	<b>7</b>
<b>Capítulo 6</b>	De la protección contra código malicioso (virus)	<b>7</b>
<b>Capítulo 7</b>	De los servicios informáticos en la red	<b>8</b>
<b>Capítulo 8</b>	Del uso de cuentas de usuario	<b>9</b>
<b>Capítulo 9</b>	Del uso del código telefónico	<b>10</b>
<b>Capítulo 10</b>	Del monitoreo del uso de los servicios informáticos	<b>10</b>
<b>Capítulo 11</b>	Del uso del Internet	<b>11</b>
<b>Capítulo 12</b>	Del uso del correo electrónico y mensajería instantánea	<b>11</b>
<b>Capítulo 13</b>	Del uso del software	<b>12</b>

## **1. INTRODUCCIÓN.**

Los Lineamientos de Seguridad Informática, son directrices que tienen como objetivo promover el buen uso y cuidado de los recursos de tecnologías de información entre el personal de este Instituto; mediante la comunicación de las medidas y formas que deben cumplir y utilizar para proteger los componentes de los sistemas informáticos del ITAIH.

Norman la forma como el ITAIH previene, protege y administra los riesgos relacionados con tecnologías de información en las instalaciones, equipos, información, servicios y soluciones informáticas.

## **2. ALCANCE.**

El personal del ITAIH y de los Sujetos Obligados del Estado, que hagan uso de nuestros servicios e infraestructura tecnológica y de comunicaciones, deben de dar cumplimiento a los Lineamientos de Seguridad Informática Institucional.

## **3. NORMATIVIDAD APLICABLE.**

Los ordenamientos jurídicos administrativos vigentes que regulan la operación de las actividades o tareas específicas a normar a través de los lineamientos de seguridad informática, entre otros, son:

- Constitución Políticas para el Estado de Hidalgo.
- Ley de Transparencia y Acceso a la Información Pública para el Estado de Hidalgo.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo.

## 4. LINEAMIENTOS.

### Capítulo 1. De la seguridad informática en la institución.

El presente documento de Lineamientos de Seguridad Informática debe ser revisado anualmente por la Dirección de Tecnologías de la Información, debe ser actualizado cuando sea necesario y todo cambio debe ser autorizado por el Consejo General de este Instituto.

Los términos y definiciones utilizados en el presente documento son:

**ITAIH:** Instituto de Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales del Estado de Hidalgo.

**DTI:** Dirección de Tecnologías de la Información.

**Usuario:** Todo empleado o funcionarios de los sujetos obligados del Estado de Hidalgo que hagan uso de los activos o servicios informáticos de la institución, para el desempeño de sus funciones, consulta o atención al servicio.

**Activo informático:** Son recursos de sistemas informáticos o relacionados con este, que son necesarios para el desempeño de las funciones del usuario, tales como equipos de cómputo, impresoras, video proyectores, teléfonos, equipos de telecomunicaciones, software, información, entre otros.

**Equipo móvil:** Es todo activo informático físico que tiene la facilidad de movilidad, como laptops, tabletas, teléfonos inteligentes, entre otros.

**Servicio informático:** Bien intangible que se proporciona para satisfacer los requerimientos de los usuarios, relacionado con el uso de activo informático.

**Medio de almacenamiento removible:** Medio externo al equipo de cómputo en el que se almacena información, como disquetes, CD, DVD, memorias (USB, SD, otras), discos externos y otros.

**Base de datos:** Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

**Derecho de autor:** Protección legal que cubre las actividades y trabajos de creación de productos de cualquier tipo que sean plasmados de forma tangible o material de conformidad con el marco aplicable en la materia. Las leyes de derecho de autor garantizan al creador el derecho exclusivo de reproducir, creación de derivados o hacer público su trabajo.

**Software institucional:** Software con licenciamiento de uso y/o propietario que puede ser instalado y utilizado por los usuarios para el desempeño de sus actividades o funciones, o para la gestión de un servicio informático otorgado por la institución.

**Software libre:** También conocido como freeware, shareware, software demo. Software gratuito proveniente de internet o cualquier otro medio que no requiere la compra de una licencia para su uso.

**Cifrar:** Técnicas bajo las cuales se transforma la información (de texto claro a texto secreto) y que solo puede ser accedida si se cuenta con las llaves o contraseñas.

**Web, www (World Wide Web):** Es una convergencia de conceptos computacionales para presentar y enlazar información que se encuentra dispersa a través de Internet en una forma fácilmente accesible.

**Virus:** Programa informático creado para producir daño en el equipo informático.

## **Capítulo 2. Del buen uso de los activos informáticos.**

**A.** Los usuarios que tengan activo informático asignado de manera personal para uso de sus funciones, son los únicos responsables de su utilización, así como también de la información contenida en los mismos, por lo que debe evitar compartirlos.

En caso de requerir compartirlo o prestar el activo informático, será solamente para cuestiones laborales y sin liberarlo de su responsabilidad.

**B.** Toda movilización de activo informático dentro o fuera de las instalaciones de la institución es responsabilidad del resguardante.

## **Capítulo 3. De la clasificación de la información.**

**A.** El dueño de un servicio informático ofrecido por la institución es responsable de la información que este servicio genera y procesa.

**B.** Todo empleado responsable de resguardo de información, debe asegurar que la información esté protegida para asegurar su integridad y confidencialidad, acorde a su clasificación. La información puede estar disponible de manera electrónica, impresa en papel, magnética, óptica y otro medio.

**C.** Todo usuario deberá hacer uso de la información a la que tenga acceso únicamente para propósitos relacionados con el cumplimiento de sus funciones, debiendo resguardar principalmente la relativa a datos personales, absteniéndose de comunicarlos a terceros sin el consentimiento expreso de la persona a la que se refieren.

**D.** Todos los usuarios que hacen uso de información clasificada como restringida o confidencial, evitarán que sea accedida por personas no autorizadas.

#### **Capítulo 4. Del intercambio de información.**

A. Toda persona que intercambie información reservada y/o confidencial con personal de ITAIH o terceras personas, debe asegurar la identidad de la persona a la que le es entregada la información, ya sea por medio físico o electrónico, dejando constancia que es procedente la entrega de información.

B. Todo convenio de ITAIH con terceras personas para compartir información reservada y/o confidencial, deberá apegarse a las disposiciones de las leyes, reglamentos y demás instrumentos normativos relacionados con acceso a la información pública y protección de datos personales.

#### **Capítulo 5. De la prestación de servicios por terceros.**

A. Todo proveedor que proporcione servicios informáticos a ITAIH y que tenga acceso a información reservada y/o confidencial, deberá apegarse a las disposiciones de las leyes, reglamentos y demás instrumentos normativos relacionados con acceso a la información pública y protección de datos personales y contar con acuerdos de no divulgación ni uso que perjudique a ITAIH.

B. Todo servicio informático otorgado por terceros debe ser monitoreado y revisado por la persona responsable de su contratación, para asegurar que se cumplan con los términos estipulados en los acuerdos o contratos de ITAIH.

#### **Capítulo 6. De la protección contra código malicioso (virus).**

A. Todo equipo de cómputo institucional debe contar con solución antivirus definida por la DTI.

B. Todo Usuario que identifique una anomalía en su equipo de cómputo deberá reportarla a la DTI.

## **Capítulo 7. De los servicios informáticos en la red.**

**A.** Todo personal son responsables del buen uso de los servicios informáticos institucionales alojados en nuestras instalaciones y en la nube, asignados para realizar sus funciones.

**B.** El personal de la DTI queda facultado para acceder a los equipos de cómputo institucionales, aun en aquellos que no están a su resguardo, para:

- la realización de revisiones en base a cumplimiento de medidas de seguridad informática como antivirus y actualizaciones,
- el inventario de software y hardware,
- por ausencia del personal en base a petición del jefe inmediato y que se requiera acceder a información y servicios en base a sus funciones,
- y a petición del Consejo General para realizar una revisión de seguridad informática y descartar uso no debido (daños intencionales a información, equipo, a personas) del equipo de cómputo, bajo previa notificación al usuario.

En caso de ausencia e imposibilidad de localizar al usuario, la notificación se realizará al jefe inmediato.

**C.** Todo titular del área con sistemas de información, es responsable de autorizar el nivel de acceso con privilegios mínimos necesarios para que el personal realice sus funciones.

**D.** Ninguna persona debe ver, copiar, alterar o destruir la información que reside en los equipos de cómputo y servidores sin el consentimiento explícito del responsable del equipo o del dueño de la información.

**E.** Todas las cuentas de usuario y su respectiva contraseña de acceso a los sistemas y servicios de información en la red del ITAIH, así como a los de telefonía, son personales, permitiéndose el uso bajo su responsabilidad, única y exclusivamente durante la vigencia de los derechos del usuario. La vigencia de las cuentas de usuarios es facultad de la DTI y del área dueña del servicio, éstas son habilitadas, suspendidas o canceladas por el área en consideración a las solicitudes, necesidades y conductas de los usuarios.



**F.** Toda utilización de herramientas tales como analizadores, escaneo y monitoreo de red, son permitidas únicamente para las funciones de administración de las tecnologías de información.

**G.** Todo hardware de telecomunicaciones (switches, enrutadores, puntos de acceso inalámbrico, entre otros) y servidores (web, FTP, correo y otros) que se requiera habilitar en la red de telecomunicaciones institucional debe ser previamente autorizado por la DTI.

**H.** A todo equipo de cómputo institucional conectado a la red del ITAIH (computadoras de escritorio y portátiles), personal autorizado por la DTI deberá de configurarlo para que pueda operar dentro de la red ITAIH, y además otorgar cuenta de usuario para acceder a los servicios de la red mencionada.

**I.** A toda persona que deje de laborar o tener relación con el ITAIH, le será cancelado su acceso de manera definitiva a los recursos informáticos institucionales. La Dirección de Administración y Finanzas comunicará a la DTI y a las demás áreas responsables de brindar servicios informáticos, toda alta, baja o cambio del personal para que se tomen las medidas correspondientes de privilegios de acceso a los servicios de red.

**J.** A todo hardware y software de uso que sean considerados de riesgo para la seguridad de los servicios informáticos institucionales, deberán ser utilizados en ambiente aislado.

## **Capítulo 8. Del uso de cuentas de usuario.**

**A.** Toda persona que requiera acceder a servicios informáticos institucionales, requerirá de una cuenta de usuario y contraseña u otro medio de autenticación. La cuenta de usuario y contraseña deberá ser asignada por el responsable del servicio.

**B.** Toda solicitud de alta, baja o cambio de privilegios de cuentas de usuario para acceder a los servicios informáticos adicionales a su perfil de puesto, debe ser solicitada a la DTI por el jefe inmediato o jefe de área demandante, debidamente justificado.

C. Todo usuario debe solicitar a la DTI, actualizar la contraseña de su cuenta de acceso a los servicios informáticos de manera periódica (al menos cada 6 meses) o cuando sospeche de su divulgación. La contraseña debe ser de al menos 8 caracteres alfanuméricos y que sea fácil de recordar.

D. Cuando se requiera acceder a información de un equipo de cómputo y/o cuenta de correo institucional de una persona ausente ya sea por cuestiones de salud, por estar comisionado a actividades fuera de su área de trabajo u otro motivo no especificado, el responsable del área correspondiente deberá solicitar a la DTI que se brinde el acceso al equipo y/o servicio o sistema informático para poder dar continuidad a algún proceso institucional.

Personal de la DTI únicamente proporcionará acceso al responsable del área correspondiente que lo haya solicitado a efecto de que sustraiga la información necesaria.

Si una persona deja de laborar en la Institución o cambia de puesto, el jefe inmediato podrá solicitar a la DTI el acceso al equipo institucional que este tenía asignado, el cual es concedido para que sustraiga la información pertinente.

## **Capítulo 9. Del uso del código telefónico.**

A. A todo usuario con servicio de telefonía se le asignará un código telefónico, haciéndose este responsable de su uso y no divulgación.

B. Por seguridad, todo código para el servicio telefónico será cambiado a petición del usuario cuando sospeche de su divulgación, por personal responsable de administrar el servicio de telefonía institucional de la DTI.

## **Capítulo 10. Del monitoreo del uso de los servicios informáticos.**

A. Personal de la DTI realiza periódicamente inventarios de hardware y software del activo informático institucional, para dar atención a problemas de obsolescencia y revisiones de licenciamiento.

B. Además, se monitorean los servicios informáticos de red para administrar el uso del recurso informático de internet y solución de problemas.

## **Capítulo 11. Del uso de Internet.**

A. El servicio de Internet a través de las redes institucionales se considera como herramienta de trabajo, por lo que todo usuario deberá utilizarlo exclusivamente para apoyo a sus actividades en el ITAIH.

B. Todo responsable de área puede solicitar la restricción total o parcial de acceso a Internet del personal a su cargo, considerando para ello las funciones laborales que éstos realizan.

C. Para la integración de toda solución informática, el área requirente debe solicitar a la DTI evaluar y recomendar los recursos de infraestructura de cómputo y telecomunicaciones, con el fin de que se gestione los recursos necesarios para la puesta en producción de la solución.

D. Todo usuario que descargue información y archivos de Internet mediante el navegador web u otro medio como FTP y mensajería instantánea, debe de omitir descargar archivos de dudosa procedencia. Los archivos descargados de Internet pueden contener virus o software malicioso que pongan en riesgo la información del equipo de cómputo de la persona, e incluso de la Institución.

## **Capítulo 12. Del uso del correo electrónico y mensajería instantánea.**

A. El correo electrónico institucional es para uso exclusivo del empleado activo del ITAIH. Éste deberá ser utilizado sólo para realizar actividades relacionadas con sus funciones.

B. Los responsables de área deberán solicitar por los medios establecidos por la DTI, una nueva cuenta de correo electrónico para personal a su cargo.

C. El ITAIH no es garante de los contenidos expresados en texto, sonido o video, redactados y enviados mediante el correo electrónico institucional.

D. A toda persona que termine la relación laboral con el ITAIH, una vez recibida la notificación de baja por parte de la Dirección de Administración y Finanzas, se inhabilitará el servicio de correo electrónico.

De no recibir petición alguna por parte del responsable del área durante los siguientes 30 días hábiles para generar algún respaldo de los correos electrónicos contenidos en la cuenta, el contenido de la cuenta de correo inhabilitada será eliminado sin generarse ningún respaldo del mismo.

E. Toda solicitud de alta, baja o cambio de un correo institucional debe ser solicitada por el responsable del área solicitante.

F. Queda prohibido utilizar el correo electrónico para envíos de correo basura, cadenas, mercadotecnia, religiosos, propaganda política, actos agresivos e ilegales y cualquier otro contenido no apropiado para el destinatario.

G. Es responsabilidad de todo usuario del correo electrónico institucional notificar al personal de la DTI la sospecha del uso no autorizado de su cuenta.

H. Todo usuario del correo electrónico institucional, acepta que comprende y acuerda expresamente que el ITAIH, no es responsable directo e indirecto y sin limitación alguna, por pérdida de datos o de cualquier otra pérdida intangible en el servicio de correo electrónico.

I. Todo servicio de mensajería instantánea debe ser utilizado para el desarrollo de actividades concernientes al puesto del personal; donde cada persona es responsable del buen uso de este servicio.

### **Capítulo 13. Del uso del software.**

A. En todos los equipos de cómputo del ITAIH, solo se permite la instalación de software con licenciamiento vigente, ya sea de uso libre o comercial. El Personal de la DTI son los únicos facultados para la instalación del software.

**B.** Toda área del ITAIH que necesite algún software para el desempeño de sus funciones, tendrá que solicitarlo a la DTI, quien verificará los requerimientos técnicos y el completo licenciamiento para su adquisición y resguardo.

**C** Todo empleado que instale software sin licenciamiento vigente o malicioso en equipos de cómputo de la institución, se hace único responsable de las consecuencias que esto conlleve.

**D.** Las licencias de uso de software propiedad del ITAIH, otorgan a éste el derecho de emplearlas exclusivamente en los equipos asignados al personal de la institución.