PLAN DE RECUPERACIÓN DE DESASTRES Y CONTINUIDAD PARA LOS SISTEMAS INFORMÁTICOS

TLX

CONSTRUIR Y CRECER JUNTOS

GOBIERNO DEL ESTADO DE TLAXCALA 2017-2021

ITIFE

INSTITUTO TLAXCALTECA DE LA INFRAESTRUCTURA FÍSICA EDUCATIVA

Índice.

Contenido

Objetivo.

Establecer un plan de recuperación de desastres para restablecer los servicios de Tecnologías de la Información y Comunicación (TIC´s), del Instituto Tlaxcalteca de la Infraestructura Física Educativa (ITIFE), en contra de cualquier eventualidad o desastre de diversos indoles a través de estrategias y acciones a seguir.

Meta.

Contar con una guía para el personal que hace uso de las herramientas y sistemas informáticos, donde se plasman los pasos a seguir: Análisis de riesgos (antes), Medidas preventivas (durante) y Estrategias de emergencia (después) de una eventualidad, con el fin de poder disminuir el impacto negativo a la información o bienes informáticos.

Alcance.

Establecer en el presente documento estrategias y acciones las cuales deben ser acatadas por todo el personal o usuario que haga uso de la infraestructura informática y genere información que sea útil para el Instituto.

Planificación.

En este sentido se ha considerado dentro del Instituto el proceso y efecto de organizar la guía a través de las siguientes actividades:

1. **Análisis de riesgo (Antes).**

En este punto se identifica la recuperación de datos, información, hardware y software dentro del Instituto, que se tiene que proteger contra los daños ocasionados, a lo cual se clasifican en tres diferentes tipos de daños: **Menor, Moderado y Grave**.

- **Daño Menor**
  - *Datos, Información*. Se consideran:
    - No guardar un documento debido a un apagón de luz.
    - No guardar un documento debido al descuido de que el usuario final no lo hizo.
    - No guardar un documento generado por el corte de energía al desconectar la computadora por el descuido de un usuario.
    - Perdida de información en archivos o en sistemas a causa de la ejecución de variaos procesos innecesarios en un mismo tiempo.
    - Eliminar un documento por descuido del usuario.
    - Modificación del nombre del archivo sin previo aviso.
    - Modificar un documento compartido sin previo aviso, o bien sin hacer una copia de este.

  - *Hardware*. Se consideran:
    - Daño en componentes por cortes de energía repentinos.
    - Fallas en discos duros por mal formateo.
    - Daño físico en equipos portátiles por traslado del mismo sin las medidas adecuadas.

- *Software*. Se consideran:
  - Perdida de información en los equipos de cómputo o medios de almacenamiento externos, por causa de virus o software malintencionado.
  - Instalación de programas o herramientas que alteren o violen la configuración del Firewall del Instituto.
  - Modificación de la configuración de la tarjeta de red en los equipos de cómputo.
  - Modificación del lugar o la ruta de almacenamiento del documento o archivo sin previo aviso.

- **Daño Moderado**
  - *Datos, Información*. Se consideran:
    - Modificación o alteración de información a documentos vitales, para fines de lucro personal.
    - Incapacidad por enfermedad y no dejar la información de vital importancia con fácil acceso.
    - No proporcionar las cuentas de usuario y contraseña de los equipos de cómputo al jefe inmediato y no tener un respaldo de la información vital que generen del Instituto.

  - *Hardware*. Se consideran:
    - Daño por golpes no intensionales al equipo de cómputo o dispositivos de almacenamiento externos.
    - Daño por caída de líquido al equipo de cómputo o dispositivos de almacenamiento externos.
    - Daños por descargas eléctricas a componentes de los equipos de cómputo o dispositivos de almacenamiento externo.

- *Software*. Se consideran:
  - No actualizar los sistemas operativos, ocasionando un menor rendimiento o filtraciones de seguridad.
  - No actualizar el software instalado en los equipos, desaprovechando mejoras en el mismo.
  - Tener instalados programas sin licencia original sin autorización del administrador de la Oficina de informática, ocasionando lentitud en equipos y problemas de seguridad con los spyware, troyanos etc.
  - No instalar el controlador y/o software original para dispositivos externos, desaprovechando todas sus funcionalidades.

- **Daño Grave**
  - *Datos, Información*. Se consideran:
    - Perdida de información en medios de almacenamiento externos, por una mala extracción del equipo de cómputo de estos mismos.
    - Perdida de información por la creación de copias de seguridad inexistentes.
    - Sabotaje o robo de información.
    - Borrado o eliminación de información vital del Instituto sin autorización.
    - Renuncia o abandono del puesto de trabajo sin previo aviso y sin hacer entrega del equipo e información generada.
    - Por despido al personal y sin hacer una entrega recepción del equipo e información generada.

- *Hardware*. Se consideran:
    - Daños por casos fortuitos (Fuego, agua, derrumbes u otros desastres naturales), a los equipos de cómputo y sistemas informáticos del Instituto.
    - Problemas de energía eléctrica (Existen diversos sucesos que en este punto pudiesen ocurrir como, por ejemplo, que falle el suministro eléctrico por quema del transformador, por caída de postes a causa de un siniestro causado. Problemas con instalaciones eléctricas por antigüedad en las mismas.)
    - Daños por falla de algún componente al equipo de cómputo.
    - Toma de instalaciones o almacenes por lo cual se prohíbe el acceso a las mismas.

- *Software*. Se consideran:
    - Alteración o modificación en los usuarios o contraseñas de los diversos sistemas tecnológicos, con los que actualmente se genera información, los cuales podrían ser, sistema KorimaSGG, sistema SAACG.NET, sistemas de Banca Móvil, etc., por personal ajeno al Instituto y sin autorización del administrador de los sistemas.
    - Alteración o modificación en claves de acceso a base de datos, de los diferentes sistemas que se manejan, por personal ajeno al Instituto y sin autorización del administrador de los sistemas.
    - Perdida de información en los equipos de cómputo o medios de almacenamiento externos, por causa de virus.

- Cambio de claves a cualquier punto de acceso (acces point) de la red inalámbrica que se encuentra instalada en el Instituto, sin la autorización del administrador de la Oficina de Informática.
- Caducidad de licencias en software instalado, inhabilitando la edición de documentos.

2. Medidas Preventivas (Durante).

Se han establecido una serie de medidas preventivas, las cuales tienen que ser acatadas por todo el personal que haga uso de la infraestructura en TIC´S, con las que cuenta el Instituto. Esto con el fin de poder reducir las exposiciones a los riesgos y a su vez reducir el impacto negativo que pudiese tener ante cualquier eventualidad. A continuación, se enlistan:

- *Datos, Información:*
  - Acceso restringido a personas no autorizadas a información considerable.
  - Todo equipo de cómputo debe contar con un regulador de corriente, para prevenir las bajadas y subidas de energía eléctrica, evitando la perdida de información.
  - Contar con un disco duro externo para cada oficina y departamento del Instituto, para el respaldo de información.
  - Actualización de los sistemas operativos para un mejor rendimiento y seguridad.
  - A todo el personal del Instituto se le recomienda guardar su documentación en tiempo real, de ser posible cada que realicen una modificación al mismo.

- Se prohíbe la modificación o alteración de información a documentos vitales, por fines de lucro personales.
- Para la previsión de desastres naturales o bien para el resguardo seguro de la información generada, realizar la concientización del uso de plataformas de almacenamiento en la nube, por ejemplo: DROPBOX, ONEDRIVE, Correo Electrónico etc., con cuentas institucionales o propias del Instituto que sean manejadas por el administrador de la Oficina de Informática.
- Clasificación y respaldo en diversos medios de almacenamiento.
- Adecuado soporte a los equipos de cómputo, impresoras e infraestructura en TIC´S, realizando al menos dos veces al año, un mantenimiento preventivo.
- Tener un adecuado conocimiento al realizar copias de seguridad de los equipos o bien servidores, las cuales deben ser realizadas por el administrador de la Oficina de Informática.

- *Hardware:*
  - Acceso restringido al uso de los Equipos (Servidores) de personas no autorizadas.
  - Queda prohibido el uso de la infraestructura en TIC´s del Instituto a todo el personal ajeno al mismo.
  - Todo equipo de cómputo debe contar con un regulador de corriente, para prevenir las bajadas y subidas de energía eléctrica, evitando daños físicos al equipo.
  - Contar con equipos de cómputo actualizados físicamente.
  - A todo el personal del Instituto se le recomienda que antes de abrir un dispositivo de almacenamiento extraíble, (usb´s, discos duros externos, micro sd) deben ser analizados con el antivirus propio del equipo o bien ir al área de Informática para que se les analice o vacune.

- Se recomienda a todo el personal del Instituto cuidar de la infraestructura de las TIC´s (equipos de cómputo, usb, discos duros externos, impresoras, fotocopiadoras, equipos multifuncionales, escáner, etc.), ya que son la herramienta de trabajo de cada día.
- Se prohíbe el estar ingiriendo cualquier alimento o bebida cerca de los equipos de cómputo, así como deben estar instalados en un lugar apropiado con una instalación eléctrica adecuada.
- Adecuado soporte a los equipos de cómputo e infraestructura en TIC´S, realizando al menos dos veces al año, un mantenimiento preventivo.
- Restringir el acceso a los equipos de cómputo, creando cuentas con privilegios de un usuario estándar, que no pueda modificar la configuración o instalar programas no autorizados.
- Para el uso de servidores contar con un equipo UPS el cual mantendrá el equipo activo por tiempo limitado, en lo que se restablece el servicio de energía eléctrica.
- Se recomienda realizar la correcta extracción de dispositivos de almacenamiento externo, con el fin de evitar corromper la información a través del sistema operativo.

- *Software:*
  - Acceso restringido a personas no autorizadas.
  - Actualización de los sistemas operativos para un mejor rendimiento y seguridad.
  - Actualización del software instalado en todos los equipos para aprovechar todas funciones.
  - Actualización de licencias originales del software instalado en los equipos.
  - Instalación de drivers y/o software original para los dispositivos externos como impresoras, escaner, multifuncionales etc.

- A todo el personal del Instituto, que haga uso de los sistemas informáticos en sus diferentes áreas, se les recomienda hacer un manual de configuración y de procedimientos de cada una de sus actividades, respaldándolo de forma impresa y digital.
- Al responsable de los sistemas informáticos del Instituto, se le recomienda hacer un manual de instalación y configuración respaldándolo de forma impresa y digital.
- Queda prohibido a todo el personal que haga uso de la infraestructura de las TIC´s del Instituto, la instalación de software o programas que alteren o violen el Firewall sin autorización.
- Queda prohibido a todo el personal del Instituto, hacer cambios en los equipos de cómputo en la configuración de la red de internet o intranet.
- Queda prohibido el acceso a los sistemas propios del Instituto a personal no autorizado, ya que en ellos se genera información relevante.
- Adecuado soporte a los equipos de cómputo, impresoras e infraestructura en TIC´S, realizando al menos dos veces al año, un mantenimiento preventivo.
- Restringir el acceso a los equipos de cómputo, creando cuentas con privilegios de un usuario estándar, que no pueda modificar la configuración o instalar programas no autorizados.
- Evitar la sobre carga de procesos en los equipos de cómputo.
- Actualizar constantemente la base de datos del antivirus instalado en los equipos de cómputo.

Se recomienda consultar y seguir las Políticas y Lineamientos de Seguridad en Cómputo de este Instituto, en sus apartados tales como:

- Políticas de seguridad física.
- Políticas de uso adecuado.
- Políticas de cuentas.
- Políticas de acceso remoto.
- Seguridad de información sensible.
- Políticas de correo electrónico.
- Políticas de respaldos.
- Políticas para redes inalámbricas.
- Políticas de uso de direcciones IP.
- Políticas de contratación y finalización de relaciones laborales de recursos humanos en sistemas informáticos.
- Políticas de incidentes graves, entre otras.

3. Estrategias de emergencia (Después).

Siempre es de vital importancia poder contar con estrategias de emergencia ante cualquier eventualidad, ya que con esto se pretende en gran medida poder reducir el daño que provocan los desastres y mantener el servicio a los usuarios de los sistemas informáticos y todo lo que conlleva al respecto.

A lo cual se enlistan por la clasificación del tipo de daño.

- **Daño Menor**
  - *Datos, Información.*
    - Recuperación de información, del ultimo respaldo echo por el personal, área, o responsable de los sistemas informáticos del Instituto.
    - Recuperación de información perdida o extraviada, por la activación de sus cuentas de correos institucionales.
    - Recuperación de información perdida, a través de la activación de las cuentas institucionales o propias del Instituto de las herramientas usadas como DROPBOX, ONEDRIVE, Correo Electrónico, etc.
    - Recuperación de información en dispositivos de almacenamiento extraíbles, vacunando el dispositivo con el antivirus y con el uso de software especializado.
    - Recuperación de información perdida en equipos de cómputo, por daño de algún virus o software malintencionado, retirando el disco duro del equipo y recuperando la información que sea posible, utilizando herramientas y software especializado.

  - *Hardware.*
    - Limpiar el equipo de computo a causa de algún derrame de liquido, abriéndolo o desarmando las piezas.
    - Reutilizar piezas de equipos de cómputo descompuesto para poder echar a andar otro.

- *Software.*
  - Recuperación de equipos de cómputo por daño de algún virus o software malintencionado, restableciendo su configuración a un punto de restauración, restauración de fabrica o bien por el formateo del equipo e instalación de los programas.
  - Recuperar información revisando papelera de reciclaje para restaurar archivos eliminados.
  - Desinstalar de los equipos de computo programas que no hayan sido autorizados por el administrador de la oficina de informática.

- **Daño moderado**
  - *Datos, Información.*
    - Recuperación de información en dispositivos de almacenamiento extraíbles, vacunando el dispositivo con el antivirus y con el uso de software especializado.
    - Recuperación de información perdida en equipos de cómputo, por daño de algún virus o software malintencionado, retirando el disco duro del equipo y recuperando la información que sea posible, utilizando herramientas y software especializado.
    - Recuperación al acceso a los equipos de cómputo, para tener la información deseada y dar continuidad a la misma, recuperando los usuarios y contraseñas proporcionados por el personal, con el jefe inmediato o responsable de los sistemas informáticos.

  - *Hardware.*
    - Recuperación de equipos de cómputo por algún fallo físico o de hardware, cambiando o dando servicio a la piezas o componentes dañados, o bien mandándolo a garantía.
    - Tener conocimiento de las consecuencias que se pueden generar al no realizar la extracción correcta de los medios de almacenamiento externo, por lo cual se recomienda realizar los pasos necesarios y de forma correcta para llevar a cabo la extracción a través del sistema operativo.
    - Gestionar ante el área administrativas la adquisición de reguladores para cada equipo de computo.

- *Software.*
  - Recuperación de equipos de cómputo por daño de algún virus o software malintencionado, restableciendo su configuración a un punto de restauración, restauración de fabrica o bien por el formateo del quipo e instalación de los programas.
  - Recuperación de bases de datos o sistemas del Instituto, por cambios a los usuarios o contraseñas sin autorización, restaurando el ultimo respaldo echo por el personal, área, o responsable de los sistemas informáticos del Instituto.
  - Recuperación de puntos de acceso (Access point) de la red inalámbrica, reiniciándolos a estado de fábrica y volviendo a configurarlos cambiando las contraseñas de acceso.

- **Daño Grave**
  - *Datos, Información.*
    - Recuperación de información en dispositivos de almacenamiento extraíbles, vacunando el dispositivo con el antivirus y con el uso de software especializado
    - Recuperación de información perdida en equipos de cómputo, por daño de algún virus o software malintencionado, retirando el disco duro del equipo y recuperando la información que sea posible, utilizando herramientas y software especializado.

  - *Hardware.*
    - Recuperación de equipos de cómputo por algún fallo físico o de hardware, cambiando o dando servicio a la piezas o componentes dañados, o bien mandándolo a garantía.
    - Tener conocimiento de las consecuencias que se pueden generar al no realizar la extracción correcta de los medios de almacenamiento externo, por lo cual se recomienda realizar los pasos necesarios y de forma correcta para llevar a cabo la extracción a través del sistema operativo.
    - Recuperación al acceso a los equipos de cómputo, para tener la información deseada y dar continuidad a la misma, recuperando los usuarios y contraseñas proporcionados por el personal, con el jefe inmediato o responsable de los sistemas informáticos.

- *Software.*
  - Recuperación de equipos de cómputo por daño de algún virus o software malintencionado, restableciendo su configuración a un punto de restauración, restauración de fabrica o bien por el formateo del equipo e instalación de los programas.
  - Recuperación de bases de datos o sistemas del Instituto, por cambios a los usuarios o contraseñas sin autorización, restaurando el ultimo respaldo echo por el personal, área, o responsable de los sistemas informáticos del Instituto.
  - Recuperación de los sistemas informáticos del Instituto, volviendo a configurar cada uno de ellos por medio de los manuales de instalación, configuración y restaurando el ultimo respaldo echo por el personal, área, o responsable de los sistemas.
  - Difusión de este plan de recuperación, así como de las políticas y lineamientos en cómputo a todos los empleados de ITIFE.

Glosario.

TIC´s: Tecnologías de la Información y Comunicación.

Firewall: En informática, un firewall o corta fuegos es la parte de un sistema o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Access Point: Es un dispositivo que se utiliza para establecer una conexión inalámbrica entre equipos y pueden formar una red inalámbrica externa (local o internet) con la que interconectar dispositivos móviles o tarjetas de red inalámbricas.

UPS: Sistemas de alimentación ininterrumpida, en inglés uninterruptible power supply, es un dispositivo que, gracias a sus baterías u otros elementos almacenadores de energía, durante un apagón eléctrico puede proporcionar energía eléctrica por un tiempo limitado a todos los dispositivos que tenga conectados.

Software: El soporte lógico e intangible como el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema de computación.

Hardware: Se refiere a las partes físicas, tangibles, de un sistema informático, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos. Los cables, así como los gabinetes o cajas, los periféricos de todo tipo, y cualquier otro elemento físico involucrado, componen el hardware o soporte físico; contrariamente, el soporte lógico e intangible es el llamado software.

KorimaSGG: Sistema de Gestión para la Contabilidad Gubernamental.

Saacg.net: Sistema Automatizado de Contabilidad Gubernamental.