PLAN DE RECUPERACIÓN DE DESASTRES Y DE CONTINUIDAD DE LA OPERACIÓN PARA LOS SISTEMAS INFORMÁTICOS

INSTITUTO TECNOLÓGICO SUPERIOR DE ZACAPOAXTLA.

Contenido

INTRODUCCIÓN 3
ANÁLISIS Y VALORACIÓN DE RIESGOS. 4
MEDIDAS PREVENTIVAS. 6
PREVISIÓN ANTE SINIESTROS Y DESASTRES NATURALES. 7
RESPALDO Y RECUPERACIÓN. 8

INTRODUCCIÓN

Un plan de recuperación de desastres y de continuidad de la operación, también conocido como plan de contingencia informático, es una metodología para la gestión de un buen manejo y administración de las Tecnologías de la Información y las Comunicaciones, para tener un pleno dominio del soporte y el desempeño de la infraestructura informática del Instituto Tecnológico Superior de Zacapoaxtla (ITSZ).

Este plan debe tener las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las actividades de la institución. El plan se diseña para que en el caso de un siniestro se active de inmediato, permitiendo dar continuidad a las actividades y servicios de la institución.

Nuestro plan, deberá ser aplicado en primera instancia por el Centro de Cómputo, dado que en ésta área se encuentran los servidores de información, así como por cada usuario que a su vez tiene asignado un equipo de cómputo, propiedad del Instituto Tecnológico Superior de Zacapoaxtla.

Para la elaboración de este plan, se deben considerar los siguientes puntos:

- Análisis y valoración de riesgo.
  Se identifican las preocupaciones y prioridades que deberá cubrir el ITSZ, se identificará el impacto de las afectaciones y se proporcionarán las bases de una estrategia para la contingencia operativa.

- Medidas preventivas.
  Definiremos que medidas efectivas debemos tomar para controlar los diferentes accesos a los activos computaciones, consideraremos que actividades realizar para los resguardos de la información.

- Previsión ante siniestros y desastres naturales.
  Aunque un desastre natural es inevitable, si podemos estar preparados, aminorar las repercusiones y tener una pronta recuperación después del desastre. Y para definir lo verdaderamente importante se deben jerarquizar las aplicaciones.

- Respaldo y recuperación.
  Después de haber desarrollado los puntos anteriores se profundizará sobre la hipótesis del siniestro y se determinará como respuesta el modo de recuperación.

Se deberá activar el presente plan de recuperación, si se presenta alguno de los escenarios mencionados al final de este documento.

La identificación de riesgos, calificación de la probabilidad de que ocurra un riesgo, evaluación del impacto en los procesos críticos y la creación de estrategias de contingencias permite mantener la operatividad frente a eventos críticos y minimizar el impacto negativo. Los usuarios deben ser parte integral del plan de recuperación, para evitar interrupciones, estar preparados para fallas potenciales y guiar hacia una solución.

Se considerará la finalización del plan cuando se ha resuelto satisfactoriamente la incidencia presentada, y en cuanto el funcionamiento del equipo, así como el servicio brindado por él, han vuelto a la normalidad.

ANÁLISIS Y VALORACIÓN DE RIESGOS.

La pérdida total o parcial de los servicios pactados dentro del alcance del plan puede originarse por las siguientes causas:

- Delitos por computador o medios electrónicos que puedan afectar la prestación de los servicios del negocio.
- Utilización de técnicas como el acceso a los activos de información por medio de una identidad falsa, alteración de datos en forma no autorizada, negación de la ocurrencia de un acción o transacción, visualización de información no autorizada, negación del servicio y operación de las aplicaciones, obtención del acceso a la plataforma con todos los privilegios y roles que conlleven a la pérdida total o parcial de los servicios.
- Vulnerabilidades en sistemas operativos o en las aplicaciones que estén alojadas en el equipo de cómputo del ITSZ.
- Disminución en el rendimiento laboral de las personas a cargo de los diferentes departamentos.
- Exposición de accesos lógicos tales como puertas traseras, ataques asíncronos, fuga de datos, intercepción de líneas, apagado imprevisto de computadoras, ataques de negación de servicio, caballos de Troya, virus, gusanos, malware, ransomware y bombas lógicas que generen la pérdida total o parcial de los servicios del computador.
- Exposición de acceso físico tales como entradas no autorizadas, daño, vandalismo o robo de equipos o documentos, copia o visualización de información privada, alteración de equipos e información sensible, revelación al público de información privada, abuso de los recursos de procesamiento de datos que conlleven a la pérdida total o parcial de los servicios que brinda el ITSZ.

- Problemas y exposiciones ambientales tales como falla eléctrica, voltaje severamente reducido, depresiones, picos y sobre voltajes, interferencia magnética.

- Falla en el servicio de internet por parte del proveedor.

- Problemas y exposiciones en bases de datos tales como procesamiento interno erróneo, actividad errónea de administración, corrupción de los archivos, acceso indebido a la base de datos para modificarla, errores durante la generación y restauración de respaldos de información.

- Sabotaje de los procesos informáticos a causa de chantaje, fraude, descontentos, amenazas (acción disciplinaria o con despido), adictos o experimentación de problemas financieros o emocionales.

- Problemas y exposiciones en aplicación y componentes del sistema tales como código malicioso en el software, fuga de información de claves de usuarios, ataques externos para obtención indebida de claves, suplantación de usuarios externos al pedir cambio de clave, ataques externos para obtención o modificación indebida de información, inestabilidad del rendimiento del hardware o software.

- Dolo o imprudencia manifiesta por parte de personas directa o indirectamente involucrada en los procesos o servicios brindados por el ITSZ.

- Pérdida del hardware o software, propiedad del ITSZ.

- Pérdida o daño debido al cálculo o diseño erróneo del hardware y software. Falla o daño eléctrico interno.

- Daño total o parcial del hardware debido a los deterioros causados por el calor, el humo, el vapor o los medios empleados para extinguir y contener un incendio, ya sea por acción directa o indirecta, y las demoliciones que sean necesarias a consecuencia del incendio y que sean ordenadas en tal carácter por la autoridad competente.

- Combustión espontánea de algún elemento que forme parte de algún equipo de cómputo o dispositivo.

Las interrupciones del servicio o incidentes que podrían afectar el cumplimiento de las labores de los trabajadores del ITSZ pueden deberse a diferentes situaciones, tales como:

- Pérdidas de personal
  a) *Ausencia por asuntos particulares.*
  b) *Accidentes laborales.*

c) *Enfermedades.*
d) *Muerte.*
e) *Cese.*

- Cortes de servicio de transporte

MEDIDAS PREVENTIVAS.

Normas efectivas para controlar los diferentes accesos a los activos computacionales y restringirlos en caso de que se presenten.

a) Acceso físico de personas no autorizadas.
Independientemente del área de que se trate, sólo el usuario al que fue asignado el equipo de cómputo tendrá acceso total al mismo, salvo indicación directa y explícita de su jefe inmediato.

b) Acceso a plataforma Moodle y correo institucional.
El centro de cómputo administrará las cuentas de usuario y contraseñas para ambos sistemas, previa solicitud por parte de las áreas que requieran altas, bajas o modificaciones en estas plataformas.
Al recibir el nombre de usuario y contraseña, el usuario final es y será el único responsable de salvaguardar sus datos.

c) Acceso a la Red Institucional.
Sólo el personal autorizado podrá ingresar a los servicios de la red de internet institucional, el personal de Centro de Cómputo es el único que realizará la configuración necesaria para tal efecto. En caso de detectar conexiones no permitidas, se procederá a bloquear el dispositivo en cuestión de forma definitiva.

d) Acceso al área de Servidores del ITSZ (SITE).
El personal de Centro de Cómputo es el único que cuenta con el permiso para acceder a ésta área. Salvo alguna indicación por parte del personal directivo.

e) Acceso restringido a los sistemas, programas informáticos y datos.
Las áreas y departamentos del ITSZ cuentan con amplia información y sistemas diversos, para acceder a estos sistemas, se cuenta con credenciales de acceso, tales como usuarios y contraseñas, esta información será accesible por el titular del área y al menos un integrante de la misma área. Serán ambos, los únicos facultados para acceder a la totalidad de información de su departamento.

f) Uso de celulares o dispositivos inalámbricos personales.

Se permitirá el ingreso de estos dispositivos a la red del ITSZ solamente con la autorización de la Dirección General o Dirección Académica, con los permisos o restricciones que se determine en su oportunidad.

g) Uso de dispositivos de almacenamiento portátiles (Disco duro externo, memoria USB). Se utilizarán preferentemente para realizar respaldos de información y de forma general no se compartirán, para evitar cualquier posible diseminación de virus o amenazas.

Las causas más representativas que originarían cada uno de los escenarios propuestos en este **"Plan de recuperación"** se presentan en el siguiente cuadro:

Principales Procesos Identificados

Descripción	Costo/beneficio	Riesgos	Impacto en caso de suspensión	Observaciones
Servidor DHCP	Alto	Bajo	Alto	Indispensable para la operación diaria.
Servidor Web	Alto	Bajo	Alto	Plataforma Moodle, versión anterior.
Servidor Web	Alto	Bajo	Alto	Página Institucional.
Servidor Web	Alto	Bajo	Alto	Plataforma Moodle, versión nueva.
Firewall Fortinet	Alto	Bajo	Alto	Protección de la red ITSZ.
Servidor Web	Medio	Bajo	Medio	Evaluación Docente.
Servidor Web	Alto	Bajo	Alto	Sistema Integral
Servidor Web	Alto	Bajo	Alto	Control Escolar
Servidor de archivos	Medio	Bajo	Bajo	Servicio interno
PCs de las diversas áreas.	Alto	Alto	Alto	El usuario tiene injerencia directa en el nivel de riesgo.
Unidades de respaldo (discos duros externos) departamentales.	Alto	Medio	Alto	Dispositivos de alta importancia en los procesos de respaldo de información.
Dispositivos de red (switches, routers, puntos de acceso)	Alto	Bajo	Alto	Dispositivos importantes para garantizar el funcionamiento de la red.

PREVISIÓN ANTE SINIESTROS Y DESASTRES NATURALES.

Los desastres causados por un evento natural o humano, pueden ocurrir en cualquier parte, hora y lugar.

En este apartado, existen distintos tipos de riesgos, por ejemplo:

- ***Riesgos Naturales***: lluvia, huracanes, sismos, etc.
- ***Riesgos Tecnológicos***: incendios, mal funcionamiento de algún dispositivo, fallas de energía eléctrica, corte de fibra óptica.

- ***Riesgos Sociales***: robos, actos terroristas, pandillerismo.

La jerarquización consiste en el orden de los elementos que integran los sistemas de información del ITSZ, según su importancia. Esta clasificación nos permitirá definir la prioridad, incluso antes de activar un plan de desastres, podremos intentar rescatar lo que podría generar una pérdida irreparable.

Nivel	Nombre	Descripción
1	Servidores	Contienen los sistemas informáticos institucionales, así como información del personal y estudiantes.
2	Respaldos de Información	Ante cualquier eventualidad, son el medio de rescate, continuidad y puesta en marcha de la operación del ITSZ.
3	PCs de las diversas áreas.	Contienen información valiosa correspondiente a cada departamento.
4	Dispositivos de red (switches, routers, puntos de acceso)	Indispensables para el acceso a internet en las instalaciones del ITZ.

RESPALDO Y RECUPERACIÓN.

La tarea más elemental e importante que será la base de cualquier solución ante desastres en nuestra institución es el denominado **"Respaldo de información".**

Esta actividad se realizará en base a las siguientes directivas:

- ✓ El usuario es el único responsable de salvaguardar su información, y deberá realizar su respaldo de información con una periodicidad semanal, quincenal o mensual.
- ✓ El respaldo de información realizado, se mantendrá en un lugar seguro y fácilmente accesible.
- ✓ Tanto el usuario, como su jefe inmediato deberán conocer la ubicación del respaldo.
- ✓ Los respaldos de información se efectuarán en dos ubicaciones:
  1) ***Dispositivo físico****, tal como un disco duro externo, cd, dvd o memoria USB.*
  2) ***Servicio en la nube****, se recomienda el uso de* ***"Microsoft OneDrive"****, accesible desde la cuenta de correo institucional para todo el personal.*
- ✓ Respecto a la plataforma Moodle, el personal docente es el responsable de realizar el respaldo de sus cursos.

- ✓ El personal del ITSZ podrá solicitar asesoría respecto a la creación de su respaldo de información al Centro de Cómputo, misma que se otorgará oportunamente, tomando en cuenta la carga de trabajo del área.
- ✓ El resguardo del respaldo de información es responsabilidad del usuario.
- ✓ Los respaldos de información de servidores de Centro de Cómputo se realizarán semanalmente debido a su importancia en la operación del ITSZ.

Ante cualquier contingencia se aplicará el plan de recuperación dependiendo del tipo del tipo de siniestro, de acuerdo a la siguiente tabla:

Tipo	Clasificación	Consecuencias	Modo de recuperación
Incendio	Grave	Dependiendo de la magnitud la gravedad será, con pérdida total del inmueble y su contenido.	Adquisición de nuevo equipo de cómputo (servidores o PCs). Uso de último respaldo de información, obtenido por medio físico o del servicio en la nube.
Temblor	Medio	Dependerá de la escala, existe la posibilidad de que algunos equipos soporten el siniestro, por lo tanto, los equipos de cómputo y la información podrían no perderse en su totalidad.	Adquisición de nuevo equipo de cómputo (servidores o PCs). Uso de último respaldo de información, obtenido por medio físico o del servicio en la nube.
Robo	Bajo	Pérdida de equipos.	Adquisición de nuevo equipo de cómputo (servidor o PCs). Uso de último respaldo de información, obtenido por medio físico o del servicio en la nube.
Virus cibernético	Medio	Dependiendo el área donde se filtre el virus, se determinarán los daños que pueda causar.	Uso de antivirus o antimalware. En caso de pérdida de información, utilizar el último respaldo de información, obtenido por medio físico o del servicio en la nube.
Epidemia viral humana	Alto	Impedir la interacción física de los usuarios en el ITSZ.	Realizar actividades 100% en línea, salvo algunas excepciones e indicaciones por parte del área directiva y garantizar el funcionamiento de servidores, para continuar con la operación normal de la institución.

Es importante mencionar que el ITSZ cuenta con un seguro que cubre la mayoría de situaciones de riesgo mencionadas en el presente documento.

El presente plan de recuperación de desastres y de continuidad de la operación, se deberá aplicar a partir de su publicación.

Cualquier asunto no contemplado en el presente documento, será analizado y resuelto en su oportunidad por el Comité de Tecnología de Información y Comunicaciones del ITSZ.