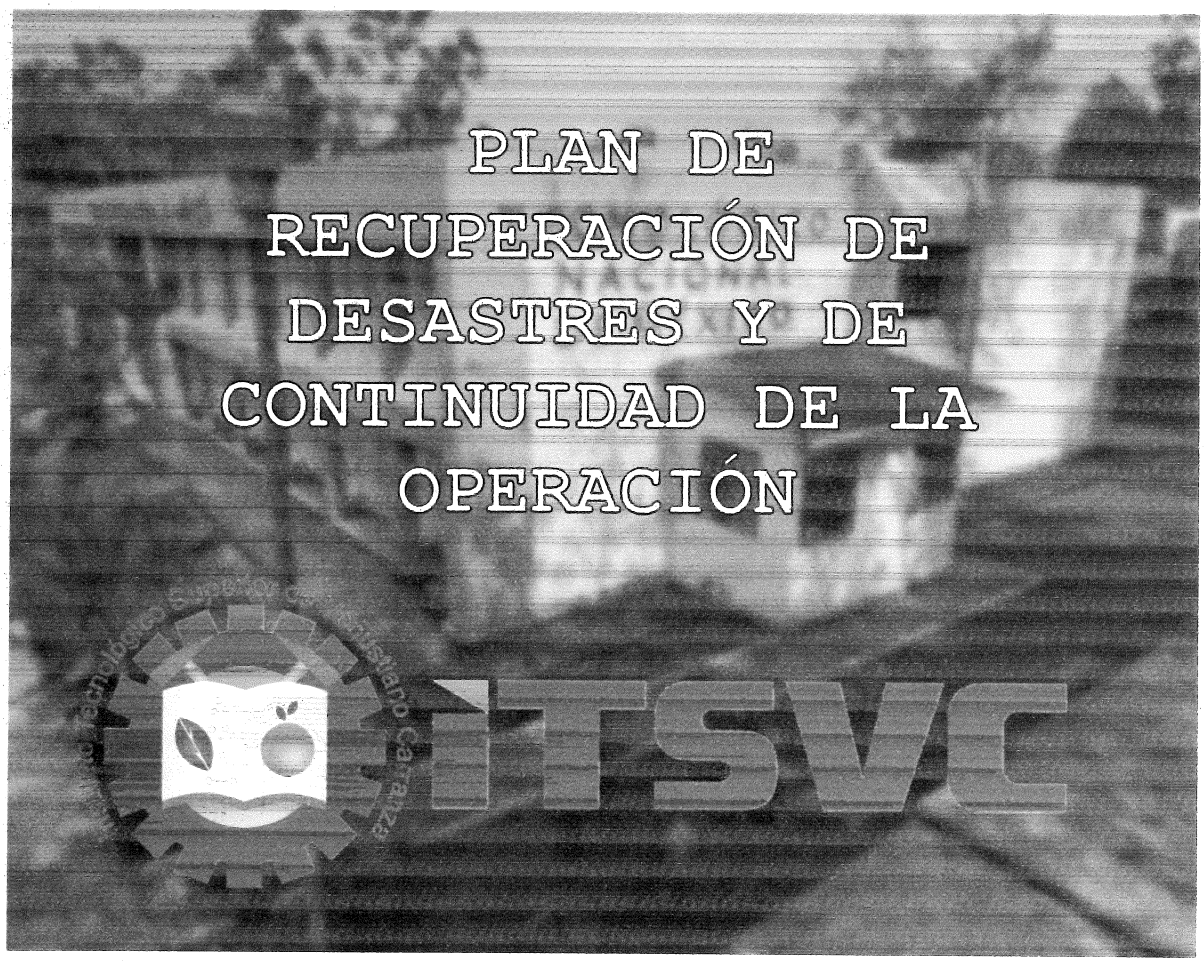

Contenido

INTRODUCCIÓN

El Plan de Recuperación de Desastres está diseñado para asegurar la continuidad de los procesos críticos de sistemas de información ante cualquier evento de desastres (falla eléctrica grave, sismo, incendio, inundación) que pueda presentarse.

Este plan proveerá de un conjunto de soluciones efectivas que podrán ser utilizadas para recuperar los procesos vitales, en los tiempos requeridos para reducir el impacto del desastre en la operación de la organización, para que esta no se vea interrumpida en el **logro de sus objetivos.**

El plan deberá ser aplicado en primera instancia por el Centro de Cómputo, dado que en ésta se encuentra la mayoría de los equipos informáticos, así como por cada usuario que a su vez tiene asignado un equipo de cómputo, propiedad del Instituto Tecnológico Superior de Venustiano Carranza.

Este plan, considera los siguientes puntos:

- **Análisis y valoración de riesgo.**
  Se identifican los riesgos y prioridades que deberá cubrir el ITSVC, se evaluaran los daños, su reparación y se dará inicio a las acciones requeridas para la recuperación de las actividades, así como la adecuación del sitio alterno.

- **Medidas preventivas.**
  Definiremos las medidas efectivas que se tomaran para controlar los diferentes accesos a los activos de computo, 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.

- **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.

La identificación de riesgos, la evaluación del impacto en los procesos del ITSVC y la creación de estrategias de contingencias, permite mantener la operatividad frente a eventos críticos y minimizar el impacto negativo.

Se considerará la finalización del plan cuando se ha resuelto satisfactoriamente las incidencias presentadas, el funcionamiento del equipo se haya restablecido, así como el servicio brindado vuelva a la normalidad.

OBJETIVOS DEL PLAN DE RECUPERACIÓN DE DESASTRES

1) Limitar la magnitud de cualquier pérdida mediante la reducción del tiempo de interrupción de los servicios y aplicaciones.
2) Evaluar los daños, su reparación y dar inicio a las acciones requeridas para la recuperación de las actividades, así como la adecuación del sitio alterno donde se continuara con la operación.
3) Recuperar los datos y la información para el funcionamiento de las aplicaciones críticas.
4) Administrar la operación de recuperación de una manera organizada y eficaz.
5) Preparar al personal de Sistemas (Tecnologías) para responder con eficacia ante una situación de desastre y saber actuar ante estas situaciones.

EQUIPO DE RECUPERACIÓN Y RESPONSABILIDADES

El equipo de recuperación de desastres estará conformado por el personal responsable del **Centro de Computo**, teniendo diferentes funciones:

Subdirección de Planeación y Vinculación

↓

Jefe del Departamento de Planeación Programación y Evaluación

↓

Responsable de Centro de Computo

↓

Auxiliar de Centro de Computo

Subdirección de Planeación y Vinculación
Encargado de dirigir las acciones durante la contingencia y recuperación, el objetivo del equipo de la Subdirección es reducir al máximo el riesgo y la incertidumbre ante la situación, el titular debe tomar decisiones "clave" durante la situación de desastre

Jefe del Departamento de Planeación Programación y Evaluación
Coordinar con el Subdirector de Planeación y Vinculación y el responsable de centro de cómputo las acciones durante la contingencia, recuperación y continuidad con la operación del **ITSVC.**

Responsable de Centro de Computo
Es responsable de establecer la infraestructura necesaria para la recuperación, esto incluye todos los servidores, computadoras, comunicaciones de voz y datos, incluyendo cualquier otro elemento necesario para la restauración de los servicios.

Tiene asignadas las siguientes responsabilidades ante situación de desastre:

- Análisis de la situación
- Decisión para la activación del Plan de Recuperación de Desastres
- Iniciar el proceso de notificación a los empleados
- Seguimiento del proceso de recuperación para obtener un resultado satisfactorio y reducir en la medida de lo posible el impacto del evento de desastre sobre la operación.
- Inspeccionar la estructura física e identificar las áreas más afectadas
- Establecer la infraestructura necesaria para la recuperación, esto incluye todos los servidores, computadoras, comunicaciones de voz y datos y cualquier otro elemento necesario para la restauración de un servicio.
- Seleccionar los procedimientos que se deberán utilizar de acuerdo al evento de desastre que se haya presentado.

Auxiliar de Centro de Computo

Encargado de la realización de pruebas que verifiquen la recuperación de los sistemas críticos.

Las responsabilidades que tienen asignadas ante una situación de desastre son:

- Realizar pruebas de funcionamiento para verificar la operatividad de los sistemas y comenzar a funcionar.
- Diseñar las diferentes pruebas que se deberán realizar para los sistemas.
- Realizar pruebas que verifiquen la recuperación de los sistemas críticos.

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:

- Desastres naturales que afecten la infraestructura de la institución, así como documentación y equipo que afecte la operatividad del ITSVC.
- Alteración de datos en forma no autorizada, visualización de información no autorizada, 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 ITSVC.
- Fuga de datos, intercepción de líneas, apagado imprevisto de computadoras, virus: caballos de Troya, 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, 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 ITSVC.
- Problemas y exposiciones ambientales tales como falla eléctrica, voltaje severamente reducido, picos y sobre voltajes e 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, acceso indebido a la base de datos para modificarla, errores durante la generación y restauración de respaldos de información.
- Fuga de información de claves de usuarios, ataques externos para obtención indebida de claves, inestabilidad del rendimiento del hardware o software.
- Pérdida del hardware o software, propiedad del ITSVC.
- 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.

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.**
Sólo el usuario al que tenga 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 ITSVC (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 ITSVC cuentan con amplia información, 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 ITSVC solamente con la autorización de la Dirección General o Subdirección de Planeación y Vinculación.

g) **Uso de dispositivos de almacenamiento portátiles (Disco duro externo, memoria USB).** Se utilizarán 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	Observaciones suspensión
Servidor DHCP	Alto	Bajo	Indispensable para la operación diaria.
Servidor Web	Alto	Bajo	Plataforma Moodle, versión anterior.
Servidor Web	Alto	Bajo	Página Institucional.
Servidor Web	Alto	Bajo	Plataforma Moodle, versión nueva.
Firewall Windows	Alto	Bajo	Protección de la red ITSVC. 9
Servidor Web	Medio	Bajo	Evaluación Docente.
Servidor Web	Alto	Bajo	Sistema Integral
Servidor Web	Alto	Bajo	Control Escolar
Servidor de archivos	Medio	Bajo	Servicio interno
PCs de las diversas áreas.	Alto	Alto	El usuario tiene injerencia directa en el nivel de riesgo.
Unidades de respaldo (discos duros externos) departamentales.	Alto	Medio	Dispositivos de alta importancia en los procesos de respaldo de información.
Dispositivos de red (switches, routers, puntos de acceso)	Alto	Bajo	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.

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, huelgas.

La jerarquización consiste en el orden de los elementos que integran los sistemas de información del ITSVC, 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 **ITSVC.**
3	PCs de las diversas áreas.	Contienen información valiosa correspondiente a cada departamento.
4	Documentación física que afecten a la institución	Contiene información financiera he historial de la matrícula del **ITSVC**

RESPALDO Y RECUPERACIÓN.

Respaldo de información es la tarea elemental para salvaguardar la información de los usuarios.

Se realizará de la siguiente manera:

- Es responsabilidad de cada usuario respaldar su información, de manera periódica semanal, quincenal o mensual.
- La información respaldada se mantendrá en un lugar seguro.
- Tanto el usuario, como su jefe inmediato deberán conocer la ubicación del respaldo.
- Los respaldos de información se efectuarán en dos ubicaciones:
    - ***Servicio en la nube**, accesando desde el correo institucional **"Microsoft OneDrive"**,*
    - ***Dispositivo físico**, tal como un disco duro externo o memoria USB.*
- Personal Docente podrá respaldar sus cursos desde la Plataforma Moodle
- El personal del **ITSVC** 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 **ITSVC**.

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

Tipo	Clasificación	Consecuencias	Modo de recuperación
Incendio	Grave	Dependiendo de la magnitud la gravedad pudiera ser 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 ITSVC.	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.

EVENTOS O DESASTRES

A continuación, se detalla las situaciones o eventos que pueden afectar la operación del **ITSVC.**
Se consideran eventos críticos los siguientes:

FALLA EN LA ALIMENTACIÓN DE LA ENERGIA ELÉCTRICA.

Se considera una falla en la alimentación de energía eléctrica una interrupción prolongada (más de 24 hrs.) o una variación que afecte de manera permanente la operación de la infraestructura. Para dar solución a esta situación, puede considerarse lo siguiente:

Suplir energía eléctrica del SERVIDOR mediante sistemas de emergencia (UPS y generador).

En las instalaciones, se habilitarán espacios de trabajo temporales para llevar a cabo las funciones esenciales.

Considerar un sitio alterno donde puedan ser instalados los equipos indispensables para llevar a cabo las actividades fundamentales para la operación del SITE.

Sustitución de los equipos afectados por la falla en la energía eléctrica.

INUNDACIÓN

Se considera el caso en que se presente una inundación, resultado de lluvias prolongadas o abundantes, o algún desperfecto en la tubería hidráulica y que por consecuencia pueda afectar las instalaciones del ITSVC y que a su vez ponga en riesgo la información, los equipos de cómputo, servidores y mobiliario.

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

INCENDIO

Los incendios son considerados como situaciones de emergencia con una ocurrencia más frecuente en el ambiente laboral, su magnitud puede ser desde un simple contacto, fácilmente controlable, hasta un incendio de grandes proporciones.

El ITSVC contempla que los integrantes tratarán de controlar aquellos fuegos que sean considerados como de riesgo menor y que puedan ser controlados con extintores de incendio portátiles u otros medios en los que hayan sido adiestrados y que no representen un peligro para la integridad física del personal.

Durante emergencias de incendio la prioridad máxima es proteger la salud y la seguridad de todo el personal que se encuentre dentro de las instalaciones,

HUELGA

Una vez que se inician los rumores sobre un periodo extenso de huelga:

Se procederá a realizar un resguardo general de todos los sistemas administrativos, el cual deberá ser resguardado en un sitio seguro que será definido por el Comité de Crisis.

El día que dé inicio la huelga, el personal designado por cada sistema crítico deberá trasladarse a un sitio alterno para continuar con la realización de las operaciones de los sistemas.

Una vez que se haya normalizado la situación, se realiza un resguardo de la información generada en las instalaciones provisionales y se restaurará en las instalaciones para continuar con el funcionamiento de las actividades.

DESASTRE TOTAL

Un desastre total se refiere cuando queda inoperante la mayor parte de los recursos con los que cuenta, para desempeñar sus actividades. Para reducir el impacto de este evento sobre la operación del SITE, es recomendable realizar las siguientes actividades:

Ubicar un sitio alterno para reanudar las operaciones.

Restaurar los sistemas necesarios dando prioridad al proceso de manejo de incidentes.

Implementar un servidor de VPN (Servidor Virtual) para el uso de aquellos usuarios que no puedan trasladarse al nuevo sitio de operaciones.

Elaborar respaldos de los datos generados en las nuevas instalaciones de forma diaria.

Elaborar reporte de daños.

PARA TODOS LOS CASOS DE DESASTRE MENCIONADOS SE DEBERÁ SEGUIR LO SIGUIENTE:

La prioridad principal en una situación de desastre es evacuar de forma segura a todo el personal para evitar daños que atenten contra la vida de éstos.

En un evento de desastre los procedimientos de emergencia deben ser seguidos de forma inmediata:

- Establecer procedimientos de evacuación del personal y de la comunidad estudiantil, mediante el uso de salidas de emergencia que permitan salvaguardar la integridad física de todo el personal.
- Después del acontecimiento y cuando las autoridades encargadas de efectuar el protocolo lo consideren seguro, deberán evaluar el impacto en coordinación con el **equipo de recuperación y responsabilidades** sobre las instalaciones y la operación del ITSVC.

INSTALACIONES DE RESERVA

Las instalaciones alternativas que permitirán la continuidad en la operación de deberán tener los recursos indispensables para que el equipo pueda retomar las actividades y continuar con la operación:

- Instalaciones eléctricas
- Mobiliario (sillas, escritorios, papelería, archiveros)
- Equipo de cómputo (PC, equipos portátiles, servidores)
- Líneas telefónicas
- Internet
- Impresora
- Software requerido para las actividades.

Cualquier asunto no contemplado en el presente documento, será analizado y resuelto en su oportunidad por la parte directiva del ITSVC.

Elaboro	Reviso	Autorizo
Tomas Joseth Maldonado López Encargado del centro de cómputo	Jorge A. Olmedo Olmos Subdirector de Planeación y Vinculación	Gladys Valderrabano Gutiérrez Enc. del Despacho de la Dirección General del ITSVC

Esta es la última hoja del **PLAN DE RECUPERACIÓN DE DESASTRES Y DE CONTINUIDAD DE LA OPERACIÓN del ITSVC.**