



PLAN DE RECUPERACIÓN DE DESASTRES EN MATERIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES PARA EL EJERCICIO FISCAL 2025 DEL COMITÉ ADMINISTRADOR POBLANO PARA LA CONSTRUCCIÓN DE ESPACIOS EDUCATIVOS

I. INTRODUCCIÓN

1.1 Contenido

El Plan de Recuperación de Desastres en materia de tecnologías de la información y comunicaciones del Comité Administrador Poblano para la Construcción de Espacios Educativos (CAPCEE) es un documento en el que se establecen las acciones que se llevarán a cabo para restaurar o mantener la operatividad de los sistemas, datos y aplicaciones de la Entidad en caso de presentarse algún evento como fenómenos geológicos e hidrometeorológicos, errores humanos o fallos técnicos.

1.2 Alcance

El presente Plan es aplicable a todos los sistemas de información (software), infraestructura tecnológica (hardware) e información almacenada en los equipos de la Entidad que funcionan como servidores de archivo, en apego a los Lineamientos en materia de Seguridad Informática del Comité Administrador Poblano para la Construcción de Espacios Educativos.

1.3 Definiciones

Para los efectos de los presentes Lineamientos, se entenderá por:

Aplicación: Cualquier programa computacional de uso específico para el Comité que se encuentre en operación y que puedan desarrollarse de manera interna por las personas servidoras públicas, por terceros de manera particular para el Comité o ser licenciadas por uno o varios proveedores contratados para tal efecto.

Brigada: Grupo de personas que se organizan dentro de un inmueble, capacitadas y adiestradas en funciones básicas de respuesta a emergencias tales como: primeros auxilios, combate a conatos de incendio, evacuación, búsqueda y rescate; designados como encargados del desarrollo y ejecución de acciones de prevención, auxilio y recuperación, con base en lo estipulado en el Programa Interno de Protección Civil del inmueble.

Comité: Comité Administrador Poblano para la Construcción de Espacios Educativos.

Departamento TI: Departamento de Tecnologías de la Información adscrito a la Dirección de Desarrollo y Seguimiento Operacional del Comité.

Desastre: Al resultado de la ocurrencia de uno o más agentes perturbadores severos y o extremos, concatenados o no, de origen natural, de la actividad humana o aquellos provenientes del espacio exterior, que cuando acontecen en un tiempo y en una zona determinada, causan daños y que por su magnitud exceden la capacidad de respuesta de la comunidad afectada.





Desastres naturales: eventos de origen natural como incendios, inundaciones, terremotos, tormentas, etc., que pueden afectar la infraestructura de TIC.

Dirección: Dirección de Desarrollo y Seguimiento Operacional del Comité.

Equipo de Cómputo: Dispositivo electrónico propiedad del Comité asignado a la persona servidora pública capaz de almacenar información, procesar datos y entregarle los resultados de la información procesada.

Error humano: se refiere a acciones o decisiones no intencionales realizadas por personas que resultan en fallos, desviaciones de las normas o consecuencias no deseadas dentro de un sistema o proceso tecnológico.

Evento: se refiere a cualquier ocurrencia o incidente que afecte el funcionamiento normal de los sistemas informáticos o la seguridad de la información.

Fallos técnicos: se refiere a cualquier error, defecto o problema que impida el correcto funcionamiento de un sistema informático, hardware o software como interrupciones del servicio de internet, fallas en servidores o equipos, errores en el software, problemas de conectividad, etc.

Fenómeno Geológico: Agente perturbador que tiene como causa directa las acciones y movimientos de la corteza terrestre. A esta categoría pertenecen los sismos, las erupciones volcánicas, los tsunamis, la inestabilidad de laderas, los flujos, los caídos o derrumbes, los hundimientos, la subsidencia y los agrietamientos.

Fenómeno Hidrometeorológico: Agente perturbador que se genera por la acción de los agentes atmosféricos, tales como: ciclones tropicales, lluvias extremas, inundaciones pluviales, fluviales, costeras y lacustres; tormentas de nieve, granizo, polvo y electricidad; heladas; sequías; ondas cálidas y gélidas; y tornados.

Hardware: Conjunto de elementos materiales que constituyen un equipo de cómputo, incluye los dispositivos electrónicos y electromecánicos, circuitos, cables, tarjetas, gabinetes, periféricos de todo tipo y otros elementos físicos.

Infraestructura: Conjunto bienes informáticos, cableado, equipos de cómputo, conmutadores telefónicos y otros equipos de naturaleza tecnológica, así como sus sistemas operativos, que funcionan como un sistema o como un conjunto de subsistemas, cuya operación y administración es competencia del Departamento de Tecnologías de la Información.

Lineamientos: Lineamientos en Materia de Seguridad Informática del Comité Administrador Poblano para la Construcción de Espacios Educativos.

Seguridad Informática: Conjunto de medidas necesarias para mantener la integridad, disponibilidad, confidencialidad y autenticidad de la información manejada en forma electrónica.

Servidor (hardware): Un servidor basado en hardware es una máquina física integrada en una red informática en la que, además del sistema operativo, funcionan uno o varios servidores basados en software. Una denominación alternativa para un servidor basado en hardware es "host" (término





inglés para "anfitrión"). En principio, todo equipo de cómputo puede usarse como "host" con el correspondiente software para servidores.

Sistema de Información: Conjunto ordenado de mecanismos que tienen como fin la administración de datos y de información, de manera que puedan ser recuperados y procesados fácil y rápidamente.

Software: Conjunto de instrucciones, programas o aplicaciones usados por una computadora para hacer una determinada tarea.

TIC: Tecnologías de la Información y Comunicación, mismas que se entienden como un conjunto de técnicas, desarrollos y dispositivos avanzados que integran funcionalidades de almacenamiento, procesamiento y transmisión de información.

II. RECURSOS INFORMÁTICOS

2.1 Equipos de Cómputo

A continuación, se listan los equipos catalogados como servidores que concentran información de las áreas que integran el Organismo. El Comité Administrador Poblano para la Construcción de Espacios Educativos cuenta con equipos de escritorio, que funcionan como pequeños servidores de archivos que guardan información de sus respectivas áreas.

- **DIRECCIÓN DE DESARROLLO Y SEGUIMIENTO OPERACIONAL**

ÁREA	USUARIO	UBICACIÓN
Adjudicaciones	ILIANA	\\Pc1coradj\ VARIAS CARPETAS
Prog. Acciones	RICARDO	\\pc167ddso\ VARIAS CARPETAS
SubDirProgyCoor	CINTHIA	\\PCSUBDIRPYC\ VARIAS CARPETAS
SubDirPlanySeg	D. MUNGUIA	\\PC68PLA\SUBDIRPLASEG\ VARIAS CARPETAS
Exp. Unitarios CARPETAS	ENRIQUE	\\pcserexpuni\D\DIGITALIZADOS\ VARIAS
Exp. Unitarios	ENRIQUE	\\pcserexpuni\expuni2021\ VARIAS CARPETAS
CEI	ADRIANA	\\PCADRIANA\COMPARTIDA\ VARIAS CARPETAS
CEI	JOSE LUIS	\\PCJOSELUISK1\ VARIAS CARPETAS

- **DIRECCIÓN DE PROYECTOS Y COSTOS**

ÁREA	USUARIO	UBICACIÓN
Proyectos	DAVID	\\107PROYECTOS\ VARIAS CARPETAS
Proyectos	OSCAR	\\SRVDPYC\COSTOS\ VARIAS CARPETAS
Proyectos	ALBERTO	\\SRVDPYC\DIRECCION\ VARIAS CARPETAS
Proyectos	GUADALUPE	\\SRVDPYC\ASISTENTE\ VARIAS CARPETAS

- **DIRECCIÓN JURIDICA**

ÁREA	USUARIO	UBICACIÓN
Jurídico	JURIDICO	\\SRVJURIDICO\DIRJURIDICA VARIAS CARPETAS





- **DIRECCIÓN ADMINISTRATIVA**

ÁREA	USUARIO	UBICACIÓN
Administrativo	NANCY	\\208SRVRECMAT\FINANCIERO VARIAS CARPETAS
Administrativo	CARLOS ROA	\\SUBDIRCONTA\ SISTEMA SACG.NET (INDETEC)
Administrativo	ALEJANDRO	\\DESKTOP-6S53BI4\ VARIAS CARPETAS
Administrativo	ESTEBAN	\\SSEP-997\PROCEDIMIENTOS VARIAS CARPETAS
Administrativo	ALBERTO R.H.	\\DESKTOP-U86KVK9\ VARIAS CARPETAS

- **DIRECCIÓN DE CONSTRUCCIÓN Y SUPERVICIÓN**

ÁREA	USUARIO	UBICACIÓN
CONSTRUCCIÓN	GUSTAVO	\\SRV5CAPCEE\SHARED\SUPERVICION VARIAS CARPETAS

También se cuenta con equipos servidores como repositorios de archivos:

- **SERVIDOR (SRV1CAPCEE) (APAGADO, SOLO SE PRENDE PARA CONSULTAS HISTÓRICAS)**

Sistema Operativo: Windows Server 2003 R2
 Procesador: Intel Xeon 3.4 GHz
 Memoria RAM: 3.25 GB
 Discos Duros: 2 discos de 111 GB c/u
 Guarda información del sistema de contabilidad "SCGII GRUPO B" histórico del año (1999 – 2014).

- **SERVIDOR 4 (SRV4CAPCEE) (DISCOS DUROS LLENOS SOLO SE CONSULTA)**

Sistema Operativo: Windows Server 2008 R2
 Procesador: Intel Xeon 2.13 GHz
 Memoria RAM: 12 GB
 Discos Duros: 3 discos de 60 GB c/u Total 1.63 TB
 Guarda información de los siguientes departamentos:

Carpetas:

CONTRATOS (Departamento Jurídico / Carpeta Histórico / Carpeta 2021)

Costos (Departamento de Costos / Carpeta Histórico)

DGCapcee (Dirección General / Carpeta Histórico)

DPYC (Dirección de Proyectos y Costos / Carpeta Histórica / Carpeta 2021).

ExpedientesO (Expedientes / Carpeta Histórico)

Finanzas (Departamento de Costos y Presupuestos / Carpeta Histórico / Carpeta 2021)

INIFED (Departamento Federal INIFED / Carpeta Histórico)

Jurídico (Departamento Jurídico / Carpeta Histórico)

Licitaciones (Departamento Licitaciones / Carpeta Histórico)

OFICIALIA (Departamento de Oficialía de Partes / Carpeta Histórico)

Planeación (Departamento de Planeación / Carpeta Histórico)

Proyectos (Departamento de Proyectos / Carpeta Histórico / Carpeta 2021)

RH (Departamento de Recursos Humanos / Carpeta Histórico)

Supervisión (Departamento de Supervisión y Construcción / Carpeta Histórico / Carpeta 2021)

Transfer Construcción (Departamento de Supervisión y Construcción / Carpeta 2021)





UDAPI (Subdirección de Planeación y Seguimiento / Carpeta Histórico)

UDAPI2 (Subdirección de Planeación y Seguimiento / Carpeta Histórico / Carpeta 2021)

A este servidor se conectan alrededor de 40 usuarios solo para consultas.

- **SERVIDOR (SRVOPUS)**

Sistema Operativo: Windows Server 2012 R2

Procesador: Intel Xeon 3.31 GHz

Memoria RAM: 32 GB

Discos Duros: 1 discos de 2 TB

Guarda información de los siguientes departamentos:

Costos y Presupuesto (Presupuestos de obras)

Supervisión y Construcción (Estimaciones de obras)

A este servidor se conectan alrededor de 35 usuarios.

- **SERVIDOR (SRVCAPCEE)**

Sistema Operativo: Windows Server 2012 R2 Standard

Procesador: Intel Xeon 1.76 GHz

Memoria RAM: 8 GB

Discos Duros: 1 discos de 2 TB

Guarda información del área de Expedientes Unitarios

Se encuentran digitalizados los expedientes del 2011 al 2016 para consultarlos de manera digital a través de una base de datos y su aplicativo Alchemy. Se conectan alrededor de 20 usuarios.

- **SERVIDOR (SRVPROYECTOS)**

Sistema Operativo: Windows Server 2012 R2 Standard

Procesador: Intel Core i3-4150 3.5 GHz

Memoria RAM: 10 GB

Discos Duros: 1 discos de 500 GB / 1 disco de 2 TB / 1 disco de 3 TB externo

Guarda información de todos los planos realizados en CAPCEE

A este servidor se conectan alrededor de 20 usuarios.

Actualmente se ocupa el disco de 2 TB ya que el disco de 3 TB ya se llenó.

- **SERVIDOR (SRV5CAPCEE)**

Sistema Operativo: Windows Server 2016 Standard

Procesador: Intel Core i3-4150 3.5 GHz

Memoria RAM: 16 GB

Discos Duros: 1 discos de 500 GB / 1 disco de 2 TB

Guarda información de la Dirección de Supervisión y Construcción

A este servidor se conectan alrededor de 30 usuarios.

- **SERVIDOR (SRVJURIDICO)**

Sistema Operativo: Windows Server 2016 Standard

Procesador: Intel Core i3-4150 3.5 GHz

Memoria RAM: 24 GB

Discos Duros: 1 discos de 500 GB / 1 disco de 2 TB





Guarda información de la Dirección de Jurídica
A este servidor se conectan alrededor de 10 usuarios.

- **SERVIDOR (SRVDDSO1)**

Sistema Operativo: Windows Server 2016 Standard
Procesador: Intel Core i3-4150 3.5 GHz
Memoria RAM: 16 GB
Discos Duros: 1 discos de 500 GB / 1 disco de 2 TB
Guarda información de la Dirección de Desarrollo y Seguimiento Operacional
A este servidor se conectan alrededor de 10 usuarios.

- **SERVIDOR (SRVDPYC)**

Sistema Operativo: Windows Server 2016 Standard
Procesador: Intel Core i3-4150 3.5 GHz
Memoria RAM: 4 GB
Discos Duros: 1 discos de 500 GB / 1 disco de 1 TB
Guarda información de la Dirección Proyectos y Costos
A este servidor se conectan alrededor de 10 usuarios.

III. ACCIONES A REALIZAR ANTE UN EVENTO O SITUACIÓN DE DESASTRE

3.1 Fenómeno Geológico

Los sismos son fenómenos causados por movimientos de la corteza terrestre y como resultado de esto, se producen vibraciones que se propagan en todas direcciones y que la población percibe como sacudidas o balanceos. México está ubicado en una zona de alta sismicidad, por lo que en caso de presentarse un evento de esta naturaleza, el Departamento TIC deberá:

- a) Apegarse a lo establecido en el Programa o Plan de Protección Civil Institucional.
- b) Realizar una inspección al hardware, software y periféricos, cuando la brigada de protección civil determine que sea seguro.
- c) Desconectar el suministro eléctrico para reducir el riesgo de que los equipos sufran algún daño.
- d) Analizar la magnitud de los daños.
- e) Informar a la Dirección sobre los daños que presenten el hardware, software y periféricos.
- f) Iniciar acciones de recuperación.
- g) Elaborar un reporte sobre las acciones realizadas.

3.2 Fenómeno Hidrometeorológico

Las lluvias favorecen el medio ambiente, alimentan los ríos subterráneos y ayudan a limpiar la ciudad, pero cuando son excesivas pueden ocasionar graves daños y pérdidas. Nuestro país está expuesto a los efectos de las lluvias y ciclones tropicales. Las inundaciones se refieren a la presencia de agua donde habitualmente no la hay, como consecuencia de marea de tormenta o falla de una estructura hidráulica; por la caída de lluvia intensa durante muchas horas o días; por tirar basura en las calles que tapa las coladeras, por tirar cascajo o basura en barrancas o ríos,





todos estos desperdicios impiden que el agua siga su cauce natural y favorece su desbordamiento. Para este caso, el Departamento TIC deberá:

- a) Apegarse a lo establecido en el Programa o Plan de Protección Civil Institucional.
- b) Realizar una inspección al hardware, software y periféricos, cuando la brigada de protección civil determine que no haya energía eléctrica y sea seguro.
- c) Desalojar el agua estancada en coordinación con la brigada de protección civil.
- d) Desconectar los equipos para evitar que sufran algún daño.
- e) Analizar la magnitud de los daños.
- f) Acondicionar un espacio físico limpio y sin humedad para la colocación de los equipos.
- g) Informar a la Dirección sobre los daños que presenten el hardware, software y periféricos.
- h) Iniciar acciones de recuperación.
- i) Elaborar un reporte sobre las acciones realizadas.

3.3 Incendios

Un incendio es un fuego de grandes proporciones que está fuera de control, que puede originarse de manera súbita o gradual; provoca serios daños materiales, interrumpe servicios y afectan el ambiente, y en ocasiones causan la muerte de muchas personas. Las causas más comunes son los cortocircuitos, flamazos por fugas de gas, dejar velas o veladoras encendidas, olvidar alimentos sobre la estufa encendida y por almacenar combustibles cerca de fuentes de calor o de aparatos eléctricos. En menor medida, por arrojar colillas de cigarro a botes de basura, fogatas y el uso de cohetes. En este caso, el Departamento TIC deberá:

- a) Apegarse a lo establecido en el Programa o Plan de Protección Civil Institucional.
- b) Realizar una inspección al hardware, software y periféricos, cuando la brigada de protección civil determine que sea seguro.
- c) Desconectar los equipos para evitar que sufran algún daño.
- d) Analizar la magnitud de los daños.
- e) Acondicionar un espacio físico limpio y sin humedad para la colocación de los equipos.
- f) Informar a la Dirección sobre los daños que presenten el hardware, software y periféricos.
- g) Iniciar acciones de recuperación.
- h) Elaborar un reporte sobre las acciones realizadas.

3.4 Fallo en el suministro eléctrico

Los cortes de corriente eléctrica por muy pequeños que sean pueden causar daños físicos o pérdidas de datos en los equipos de cómputo. Los sistemas de alimentación ininterrumpida (UPS) son aparatos diseñados para mantener el equipo de cómputo encendido en caso de interrupción eléctrica, el tiempo que se mantiene encendido un equipo varía según el modelo y la batería del UPS, el objetivo principal es permitir al administrador apagar los servidores de manera correcta y con esto evitar la pérdida de información, dañar archivos por el apagado inesperado y un daño físico en el Disco Duro. Es por esta razón que todos los equipos de cómputo servidores y equipo de escritorio cuentan con un UPS para reducir considerablemente la pérdida de información y





daños físicos en el equipo en caso de una interrupción eléctrica. En este caso, el Departamento TIC deberá:

- a) Realizar una inspección al hardware, software y periféricos.
- b) Desconectar los equipos para evitar que sufran algún daño.
- c) Analizar la magnitud de los daños.
- d) Informar a la Dirección sobre los daños que presenten el hardware, software y periféricos.
- e) Iniciar acciones de recuperación.
- f) Elaborar un reporte sobre las acciones realizadas.

3.5 Errores humanos

En el contexto de las Tecnologías de la Información y la Comunicación, los errores humanos se refieren a acciones o decisiones tomadas por personas que, de manera no intencionada, pueden llevar a fallos o vulnerabilidades en sistemas, redes o datos. Estos errores pueden ser causados por una variedad de factores, como la falta de capacitación, la fatiga, la distracción o la falta de atención a las políticas de seguridad. En este caso, el Departamento TIC:

- a) Evaluar el evento.
- b) Analizar la magnitud de los daños.
- c) Notificar al usuario sobre los daños y la probable solución.
- d) Informar a la Dirección sobre los daños que presenten el hardware, software y/o periféricos.
- e) Iniciar acciones de recuperación.
- f) Elaborar un reporte sobre las acciones realizadas.

3.6 Fallos técnicos

Los fallos técnicos en las TIC (Tecnologías de la Información y la Comunicación) pueden manifestarse de diversas maneras, afectando tanto a usuarios individuales como a organizaciones. Estos problemas pueden incluir desde fallas en dispositivos y redes hasta dificultades en la adopción y uso efectivo de las herramientas tecnológicas. Las acciones a seguir son las siguientes:

- a) Evaluar el evento.
- b) Analizar la magnitud de los daños.
- c) Informar a la Dirección sobre los daños que presenten el hardware, software y/o periféricos.
- d) Iniciar acciones de recuperación.
- e) Elaborar un reporte sobre las acciones realizadas.

IV. ACCIONES PREVENTIVAS

4.1 Respaldos de Información

La pérdida de información en forma parcial o total es un riesgo que se corre en cualquier organización, esto puede ser debido a errores involuntarios de los usuarios, fallas de hardware, fallas de software, virus informáticos, desastres naturales o bien por sabotaje.





La información que se almacena en los equipos de cómputo posee un valor de gran importancia para el CAPCEE por lo que es importante tomar medidas para reducir el impacto en el caso de pérdida de información, para estas situaciones se toma como medida preventiva los respaldos de información.

Un respaldo de información es un proceso que copia los datos importantes de un dispositivo primario en uno o varios dispositivos secundarios, para que en caso de que el primer dispositivo sufra una avería electromecánica o un error en su estructura lógica, sea posible contar con la mayor parte de la información necesaria para continuar con las actividades rutinarias y evitar pérdida generalizada de datos.

Los usuarios de los equipos de cómputo serán responsables de la información contenida en el equipo de cómputo asignado y de que esta sea debidamente respaldada. Sin embargo, a solicitud de los usuarios el Departamento de Tecnologías de la Información brinda el apoyo para la realización de respaldos de información sin ningún tipo de periodicidad.

En los equipos que funcionan como servidores de datos se hacen respaldos completos mensualmente almacenando la información en discos duros externos.

La información debe estar organizada por años de operación para poder hacer respaldos semanales del año en curso y respaldos mensuales de los años históricos de operación, así se ahorra tiempo en los respaldos y se aumenta años de vida de los discos duros del servidor.

Los respaldos mensuales solo serán de los años históricos que el área indique.

La organización de la información por años de operación la debe hacer cada área dueña de la información.

4.2 Resguardo de Información en lugar seguro

En caso de un temblor que propicie el colapso del inmueble, o un incendio deben respaldarse los discos duros en una caja de seguridad o bóveda comercial.

4.3 Acciones realizadas

El Departamento de Tecnologías de la Información instaló los siguientes aditamentos:

- Se instaló una línea directa de energía eléctrica desde la base del medidor o centro de carga principal de CFE al site (cuarto de telecomunicaciones).
- Se conectaron los 3 UPS interactivo marca EATON.
- Se pusieron contactos de energía regulada.
- Se conectaron los servidores a los contactos de energía regulada.
- El site cuenta con un respaldo de energía eléctrica por 30 min.
- En caso de corte de energía eléctrica contamos con 30 minutos para apagar los equipos correctamente y no sufrir daño.





- Todas las Unidades Administrativas cuentan con 1 disco externo de 6 TB para realizar su respaldo de su información histórica y la del año en curso.

V. ACCIONES A REALIZAR EN MEDIADO PLAZO

- Se está valorando la compra de UPS personales para PC de escritorios que fungen como pequeños servidores.
- Se instalarán 3 reguladores eléctricos marca VOGAR en las copiadoras a color para evitar daños por una variación de voltaje.
- Verificar si los pararrayos están en funcionamiento.
- Impermeabilizar todo el edificio priorizando el techo del site.
- Se está gestionando la instalación de una consola de antivirus para monitorear todos los equipos de cómputo y evitar que se infecten con virus informáticos.

Revisó

Lourdes Daniela Munguía García

Subdirectora de Planeación y Seguimiento

Validó

Rafael Morales Juárez

**Director de Desarrollo y Seguimiento
Operacional**

Elaboró

José de Jesús Correa López

Jefe del Departamento de Tecnologías de la Información

