CAASA
COMISIÓN DE AGUA
Y ALCANTARILLADO DE ACTOPAN

PLAN DE RECUPERACIÓN DE DESASTRES EN MATERIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DE LA CAASA.

1. Acerca del Plan

El Plan está diseñado para asegurar la continuidad de los procesos críticos de los servicios de cómputo, a través del encargado de Tecnologías de la Información de la Comisión de Agua y Alcantarillado de Actopan, Hidalgo (CAASA) ante cualquier contingencia (falla eléctrica grave, sismo, incendio, inundación, etc.) que pueda presentarse.

2. Propósito y Alcance del Plan

Este Plan podrá implementarse ante una situación de desastre que afecte las instalaciones y recursos de cómputo y telecomunicaciones con los que cuenta la CAASA para cumplir la misión que tiene asignada. Para llevar a cabo las actividades de recuperación, en este documento se mencionan equipos que tendrán una serie de responsabilidades, así como actividades que contribuyan a la pronta recuperación y continuidad de las actividades.

3. Actualización

El Plan debe ser revisado periódicamente por lo menos una vez al año, con el propósito de actualizar cualquier cambio que se haya presentado durante ese período.

Los siguientes aspectos deberán ser revisados en el Plan para mantenerlo actualizado:

- Cambios en el personal.
- Cambios en la misión y visión.
- Cambios en la prioridad.
- Nueva estructura orgánica.
- Procedimientos de respaldos.
- Procedimientos de recuperación.
- Plan para migración o reubicación.
- Software (sistemas operativos, utilidades y programas de aplicación).
- Hardware (servidores, periféricos, equipos de cómputo).
- Comunicaciones de red.

4. Objetivos del Plan Contingencia para Recuperación de Desastres en Materia de TIC's

a) Limitar la magnitud de cualquier pérdida de información o funcionalidad.
b) Reducción del tiempo de interrupción de los servicios y aplicaciones críticas.
c) 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.
d) Recuperar los datos y la información imprescindible para el funcionamiento de las aplicaciones críticas.
e) Administrar la operación de recuperación de una manera organizada y eficaz.
f) Preparar a los servidores públicos encargados de las tecnologías de la información de la CAASA para responder con eficacia ante una situación de desastre y poder actuar sobre el proceso de recuperación.

Para lograr estos objetivos, es necesario contar con el apoyo de todos los titulares de la CAASA, además de todos aquellos integrantes que la Dirección General considere necesarios.

5. Equipos de Recuperación y sus responsabilidades

Los equipos de recuperación estarán formados por los servidores públicos necesario en la activación y desarrollo del Plan. Cada equipo tiene funciones y procedimientos que deberán desarrollar, considerando lo establecido en este Plan.

a) Equipo Director

Es el encargado de dirigir las acciones durante la contingencia y recuperación. El objetivo del equipo director es reducir al máximo el riesgo y la incertidumbre en la atención de la situación de que se trate. Deberán de tomar las decisiones "clave" durante la situación de desastre.
Este Equipo estará integrado por el Director General y los o las titulares de las Secretaría Técnica, Subdirección de Administración y Finanzas y Órgano Interno de Control.

Las responsabilidades que deberá observar este Comité en una situación de desastre son:

• Analizar la situación.

• Activar el Plan de recuperación de desastres.

• Notificar a los servidores públicos de la CAASA a través de las diferentes instancias responsables sobre la situación de crisis que se esté viviendo en ese
momento.

• Dar seguimiento al proceso de recuperación, definiendo los tiempos necesarios para tener un resultado satisfactorio y reducir el impacto del desastre sobre la operación y el estado financiero de la CAASA.

b) Equipo de Recuperación y Pruebas (Encargado de Tecnologías de la información de la CAASA)

Es el responsable de restablecerla infraestructura necesaria para la recuperación. Esto incluye todos los servidores, computadoras, redes de voz y datos, incluyendo cualquier otro elemento necesario para la restauración de los servicios. También es el encargado de la realización de las pruebas que verifiquen la recuperación de los sistemas críticos.

Este equipo estará integrado por personal de Tecnologías de la información, que cuente con la experiencia necesaria en el manejo de sistemas, hardware, software y telecomunicaciones.

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

a) Inspeccionar la estructura física e identificar las áreas más afectadas.
b) Establecer los medios y los procesos necesarios para la recuperación, esto incluye los servidores, las computadoras, las redes de comunicación de voz y datos y cualquier otro elemento necesario para la restauración del servicio de la infraestructura de cómputo.
c) Elegir los procedimientos que se deberán utilizar de acuerdo con el tipo de contingencia que se haya presentado.
d) Diseñar las diferentes pruebas que se deberán aplicar para analizar todos los sistemas.
e) Realizar las pruebas de funcionamiento necesarias para verificar la operatividad de los sistemas y ponerlos a punto para su óptimo funcionamiento.

6. Acciones a realizar ante una contingencia

La prioridad principal en una contingencia es evacuar de forma segura a todos los

servidores públicos de la CAASA a para evitar cualquier suceso que atente contra la seguridad física de ellos.

En un evento de interrupción física mayor, los procedimientos de emergencia deben ser implementados de forma inmediata.

Se deben establecer procedimientos de evacuación de la CAASA mediante el uso de salidas de emergencia que permitan salvaguardar la integridad física del personal.

Después del acontecimiento, el Director General deberá evaluar el impacto sobre las instalaciones y la operación de la CAASA, y con ello tomar las decisiones que correspondan, informando al encargado de Tecnologías de la Información para llevar a cabo los procesos de respaldo y posterior recuperación de la información.

7. Procedimientos que deberá realizar el encargado de Tecnologías de la Información.

Analizará la índole y la magnitud del problema.

Si es seguro hacerlo, deberá desconectar el suministro eléctrico a las instalaciones del Instituto, para reducir el riesgo de daño en los equipos eléctricos.

Hará una evaluación inicial e informará al Director General sobre la magnitud de los daños a la infraestructura, así como a los equipos de cómputo, servidores, documentación y situación personal.

También informará sobre las medidas que se tomarán para reducir el impacto del desastre sobre las áreas de operación de la CAASA para que el Director Genera pueda decidir la puesta en marcha del Plan de recuperación de desastres.

8. Escenarios de Recuperación

Las situaciones y eventos críticos que pueden afectar la operación de la CAASA y las acciones que se deberán tomar son las siguientes:

a) Falla en el suministro de energía eléctrica

Se considerará una falla la interrupción prolongada de energía eléctrica por más de 24horas. Para poder solucionar esta situación se considerará lo siguiente:

Sustituir la alimentación de energía eléctrica de la CAASA mediante la instalación de sistemas de emergencia como UPS's o generadores.

• En la CAASA se habilitarán espacios de trabajo temporales, para poder realizar las funciones esenciales del mismo.

• También se deberá considerar un sitio alterno donde puedan ser instalados equipos indispensables para realizar las actividades fundamentales en la operación de la CAASA.

• Finalmente se considerará la sustitución de los equipos que se hayan dañado por la falla en la energía eléctrica.

b) Inundaciones

En caso de 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 de la

CAASA, y que a su vez ponga en riesgo la integridad física de la información, los equipos de cómputo, servidores y mobiliario.

Para dar solución a esta situación, antes, durante y después de que ocurra, se deberá realizar lo siguiente:

Antes

• Asegurar que la Dirección General esté debidamente constituido y conozca los procedimientos de recuperación establecidos en el presente documento.

• El encargado de Tecnologías de la Información deberá asegurarse que los sistemas de comunicación, aviso y alarma estén disponibles en todo momento.

• El Director General deberá establecer comunicación con las entidades de apoyo externo por parte de Tecnologías de Información para que puedan brindar ayuda en caso de presentarse un desastre de este tipo.

• El encargado de Tecnologías de la Información realizará una inspección de las áreas físicas para determinar aquellas que son susceptibles a inundaciones.

• Es responsabilidad del área de servicios generales realizar revisiones periódicas para examinar los sistemas de drenaje de los edificios, del terreno y verificar los sistemas de alcantarillados.

• La Dirección General debe hacer una revisión periódica del Plan de Recuperación de Desastres a fin de mantenerlo actualizado.

Durante

• La Dirección General debe indicar cuándo deberá ser puesto en marcha el Plan de Recuperación de Desastres, además deberá indicar a las autoridades que correspondan sobre la magnitud de la emergencia y la acciones que se tomarán al respecto.

• Impartirá instrucciones al Equipo de Recuperación y Pruebas.

• Los directores, jefes de los departamentos y el personal a cargo, deberán guardar los documentos importantes en lugares seguros que no puedan ser afectados por el agua, además se encargarán de coordinar el movimiento de equipos a lugares donde puedan estar protegidos y permanecer con un material impermeable en caso de no poder ser removidos de su ubicación física.

• El encargado de Tecnologías de la Información, deberá reubicar en un sitio seguro todos los equipos de cómputo, servidores y mobiliario que se encuentren dentro de las instalaciones de la CAASA hasta donde sea posible, además deberá cerrar todas las válvulas de servicios como gas, agua y fuentes que no sean imprescindibles.

• El encargado de Tecnologías de la Información deberá inspeccionar todas las áreas e informará a la Dirección General sobre cualquier condición insegura que exista en las instalaciones que corresponden a los edificios de la CAASA además se encargará de asegurar que los documentos esenciales estén protegidos en bóvedas o con cualquier otro lugar o sitio, que evite sean dañados, destruidos o extraviados.

• El encargado de Tecnologías de la Información se encargará de notificar a la Dirección General cualquier situación que atente contra la vida o seguridad de las personas.

Después

• El encargado de Tecnologías de la Información coordinará las labores de limpieza y desinfección para el control de plagas o epidemias en las áreas afectadas por la inundación además evaluará las condiciones de la CAASA, determinando en cuáles áreas existe la posibilidad de reanudar las actividades, también coordinará una inspección para determinarlas mejoras que se pueden realizar en los sistemas de drenaje y estructuras, con el fin de prevenir emergencias futuras.

• El encargado de Tecnologías de la Información se encargará de coordinar las labores de restauración de las áreas afectadas por la inundación.

• El Subdirector de Administración y Finanzas, con la autorización del Director General deberá informar a las autoridades del Municipio de Actopan, Hidalgo, los resultados de la evaluación de los daños y todos los informes que sean necesarios, además será el responsable de difundir la información a la comunidad de la CAASA.

c) Sismos o Terremotos

Considerando que el Municipio de Actopan, Hidalgo, es paso de la ruta México Laredo, es de tomar en cuenta que en caso de sismos o terremotos se deben considerar las siguientes actividades para enfrentar este tipo de eventos.

Antes

• Asegurar que Dirección General conozca los procedimientos de recuperación establecidos en el presente documento.

• La Subdirección de Administración y Finanzas, a través de su Área de Mantenimiento, deberá realizar revisiones periódicas para asegurar que los sistemas de comunicación, aviso y alarma estén disponibles en todo momento.

• La Dirección General deberá establecer comunicación con las entidades de apoyo externo por parte de la CAASA para que puedan brindar ayuda en caso de presentarse un desastre de este tipo.

• La Dirección General, deberá hacer una revisión por lo menos anual de los procedimientos establecidos en este plan.

• El encargado de Tecnologías de la Información, coordinará un conjunto de pláticas o conferencias informativas sobre las acciones a tomar en caso de sismos o terremotos, con el fin de concientizar al personal en cómo debe actuar ante una situación de desastre de este tipo, así como hacer de su conocimiento los procedimientos descritos en este plan para reducir el impacto de un sismo o terremoto sobre las instalaciones y recursos propiedad de la CAASA.

• Los Directores, subdirectores y demás titulares que integran a la CAASA serán los responsables de mantener su área de trabajo ordenada, limpia y segura, además pedirán información a la Subdirección de Administración y Finanzas sobre equipo o medidas para protección contra sismos. De igual forma establecerán procedimientos para almacenar de forma segura los materiales o equipos.

Durante

• Los integrantes de la CAASA deberán evacuar las instalaciones cuando la alarma de emergencia este activada, acudiendo a los puntos de reunión identificados por la Dirección de Protección Civil.

• Los integrantes de la CAASA deben conservar la calma y refugiarse fuera del edificio o en las zonas seguras, identificadas por Protección Civil.

• De no lograr abandonar las instalaciones de la CAASA deberán permanecer en sus lugares, alejados de objetos que puedan caer y dañarlos.

• Todo el personal del Instituto debe evitar correr y deberán alejarse de cristales u objetos voluminosos q u e p u e d a n caerse.

• Deben evitar utilizar velas, fósforos o cualquier otro objeto que pueda producir flama durante o después del sismo.

Es recomendable no interferir en las labores de rescate, a menos que le sea solicitada colaboración

Después

• La Dirección General y el Encargado de Tecnologías de la Información deberán realizar una inspección de los edificios de la CAASA, en la cual buscarán a personas atrapadas, heridas o lesionadas, fuentes que puedan producir algún tipo de incendio o cualquier otra situación que ponga en peligro la vida del personal.

• La Dirección General deberá informar el resultado de la evaluación de daños a la autoridad correspondiente de la CAASA, llevará a cabo la activación del presente Plan e indicará las actividades que deberá realizar Encargado de Tecnologías de la Información.

De ser necesario la Dirección General, establecerá comunicación con las entidades de apoyo externo del Municipio de Actopan, Hidalgo para el control de la situación.

d) Incendios

El Plan de Contingencias contempla que los integrantes de la CAASA tratarán de controlar aquellos incendios 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. Los incendios mayores a los descritos con anterioridad serán controlados por el Cuerpo de Bomberos del Municipio de Actopan, Hidalgo.

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 de la CAASA, para lo cual se consideran las siguientes recomendaciones, antes, durante y después de un incendio:

Antes

• Evitar la sobrecarga de líneas eléctricas.

• Evitar conectar más de un aparato eléctrico en cada toma de corriente.

• No arrojar cerillos, ni cigarros encendidos a los cestos de basura.

• Evitar fumar en áreas restringidas.

• Notificar la presencia de fugas de gas o derrames de líquidos inflamables.

• Identificar las salidas de emergencia, así como los teléfonos de servicios médicos y bomberos más cercanos.

Durante

• Los integrantes de la CAASA deben conservar la calma y avisar de inmediato a los bomberos y servicios de emergencia, éstos deberán proporcionar los datos precisos sobre el incendio (origen o causa, ubicación y características de la zona
afectada).

• Si el incendio es de poca magnitud intentar apagarlo con el extintor.

• Cubrir boca y nariz con tela húmeda, si el humo es excesivo, desplazarse rápidamente para evitar la intoxicación por inhalación de humo.

Desalojar las instalaciones de la CAASA utilizando las rutas de evacuación establecidas con anterioridad.

Después

• Los integrantes de la CAASA deberán alejarse del lugar del siniestro para evitar
entorpecer las labores de los grupos especializados en atención de emergencias.

• Los integrantes de la CAASA no deben ingresar al inmueble hasta recibir las indicaciones necesarias de los integrantes de la Dirección General.

• La Dirección General será el responsable de informar al personal de la CAASA lo sucedido y las actividades realizadas para la recuperación y continuidad de las
actividades.

e) En caso de huelga o toma de instalaciones

Cuando se inician los rumores sobre la posibilidad de un periodo extenso de huelga, se deberán realizar las acciones siguientes, para minimizar el daño que pudiera afectar el desarrollo normal de las actividades de la CAASA.

• Se procederá a realizar un resguardo general de todos los sistemas administrativos, el cual deberá ser depositado en un sitio seguro que será definido por el Director General.

• Se designará al personal necesario que será responsable de operar los sistemas administrativos que serán depositados en un sitio seguro para su resguardo.

• El día que inicie la huelga o toma de instalaciones, el personal designado por cada sistema administrativo deberá trasladarse al sitio seguro que se haya definido para continuar con la operación de los sistemas, o eventualmente también podrán ser operados desde el domicilio particular de cada una de las personas que fueron designadas para tal fin, esto como resultado de la experiencia vivida durante la cuarentena establecida por la pandemia ocasionada por el virus SARS-COV-2.
• Una vez que se haya normalizado la situación, se realizará un resguardo de la información generada en las instalaciones alternas y se restaurará en las instalaciones de la CAASA para continuar con el funcionamiento normal de las actividades.

f) En caso de desastre total

Se considera un desastre total cuando queda inoperante la mayor parte de los recursos con que cuenta la CAASA para desempeñar sus actividades. Para reducir el impacto de este evento sobre la operación de la CAASA, se deberán realizar las siguientes acciones:

• Evaluar la posibilidad de que el trabajo de la CAASA se siga llevando a cabo a distancia por parte de sus integrantes en sus domicilios particulares. De no ser así, ubicar un sitio alterno para reanudar las operaciones.

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

• Evaluar la pertinencia de la implementación de un servidor VPN para el uso de aquellos usuarios que no puedan trasladarse al nuevo sitio de operaciones y que tendrían que trabajar a distancia desde otro lugar acordado con antelación.

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

• Elaborar reporte de daños.

• Elaborar lista de materiales que se requerirán para reanudar las operaciones de la CAASA.

• Esperar indicaciones de la Dirección General para reubicar el centro de operaciones de la CAASA a través de los servidores que se hayan establecidos para tal fin.

• La Dirección General deberá decidir y dar prioridad a la restauración de aquellas actividades críticas para la operación de la CAASA.

9. Creación de un Centro de Control

El centro de control será el punto de reunión para que la Dirección General y Tecnologías de la Información puedan reunirse para evaluar la situación de desastre y tomar las decisiones adecuadas y necesarias para llevar a cabo las actividades de recuperación en la CAASA, reduciendo con ello los impactos operacionales y financieros generados por una situación de desastre.

Como primera alternativa, se puede considerar establecer el punto de reunión en el domicilio de alguno de los integrantes de la Dirección General, como segunda instancia y una vez evaluado el impacto del desastre en las instalaciones de la CAASA, las autoridades locales determinarán el sitio donde reubicarán de forma temporal al Instituto para continuar con s u s actividades.

Las instalaciones alternas deberán contar con los siguientes recursos indispensable para que la CAASA pueda retomar las actividades y continuar con su operación normal:

Instalaciones eléctricas

Mobiliario (sillas, escritorios, archiveros e insumos de oficina necesarios)

Equipos de cómputo de escritorio y portátiles, así como sus periféricos (impresoras, escáneres, copiadoras, etc.)

Líneas telefónicas.

• Conexiones a internet

• Todo el software que sea necesario para realizar las actividades.

10. Ubicación de almacenamiento de datos

En una situación de desastre es de suma importancia proteger la información, tanto los documentos físicos como todos los respaldos en electrónico que se generan en los servidores de la red local de computadoras. La CAASA debe contar con un respaldo que tiene que ser resguardado fuera de sus instalaciones y que debe ser actualizado por lo menos cada 3 meses por el responsable del Área de Redes y Servidores. A tal fin, la política de administración de servidores de la CAASA Cuenta con:

Los servicios están separados en servidores virtuales, para facilitar su administración y, de ser necesario, su recuperación.

Los servidores están configurados con almacenamiento redundante: en caso de falla de alguno de los discos, la información esta duplicada en otro, y se puede realizar reemplazo de inmediato.

La información es respaldada fuera de sitio, hacia el centro de datos de Tecnologías de la información, cada dos días. Se conservan siete respaldos, lo que permite recuperar información de hasta dos semanas hacia atrás.

11. Medidas preventivas y de neutralización ante posibles ataques cibernéticos y hackeos.

Las conexiones de red entrantes y salientes a los equipos de la CAASA (tanto a computadoras personales como servidores, equipos de videoconferencia y cualquier otro dispositivo) son validades por un firewall para permitir únicamente el flujo de tráfico a los puertos y con los protocolos aprobados. Los servidores de la CAASA, así como todas las máquinas virtuales y contenedores que se ejecutan dentro de ellos, siguen una política de instalación diaria y automática de actualizaciones no disruptivas; el área de administración de servidores debe realizar seguimiento e instalación de las actualizaciones manuales para todos los sistemas que no están integrados a las actualizaciones automáticas del sistema operativo. Todos los servicios brindados por los servidores de la CAASA mediante las máquinas virtuales y contenedores alojados en ellos son respaldados en días alternados hacia el centro de datos, manteniendo un historial de siete respaldos pasados (14 días).

12. Documentación relacionada

Se ha decidido que el presente plan solo debe contener como anexos la siguiente
documentación, considerada como necesaria, para poder realizar todas las actividades planteadas en el mismo.
Directorio telefónico de las autoridades y funcionarios de la CAASA que formaran los primeros contactos.

El listado de inventarios de los activos con que cuenta la CAASA en materia de infraestructura de cómputo y redes de voz y datos.

13. Autorización.

Plan de Recuperación de Desastres en Materia de Tecnologías de la Información y Comunicación de la CAASA; entraran en vigor al día siguiente de su aprobación.

Actopan Hidalgo a 30 de Enero del 2026

Mtro. Luis Emmanuel Bautista Guerrero
Titular del Órgano Interno de Control de la CAASA

Lic. Joselin Zúñiga López
Coordinadora del Órgano Interno de Control de la CAASA