



PLAN DE RECUPERACIÓN DE DESASTRES

DIRECCIÓN DE INFORMÁTICA



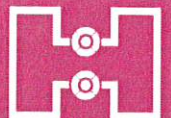
H. AYUNTAMIENTO MUNICIPAL CONSTITUCIONAL
DE TAXCO DE ALARCÓN, GUERRERO
2021 - 2024



DIRECCIÓN
DE INFORMÁTICA

Índice

1. Acerca de	1
2. Alcance	1
3. Objetivos	2
3.1 Objetivo General	2
3.2 Objetivos Específicos	2
4. Equipo De Recuperación	3
5. Procedimientos De Recuperación	4
5.1 Acciones preventivas para situación de desastres	4
5.1.1 Del servidor web y de correos	4
5.1.2 De las computadoras pertenecientes al H. Ayuntamiento Municipal	6
5.1.3 De la red de telecomunicaciones.....	7
5.1.4 Del Sistema SUINPAC.....	8
5.2 Acciones organizativas y de respuesta	9
5.2.1 Contingencia en el servidor web y de correos.....	9
5.2.2 Contingencia en alguna computadora del H. Ayuntamiento Municipal	12
5.2.3 Contingencia en la red de telecomunicaciones	16
5.2.4 Contingencia en el sistema SUINPAC.....	19
6. Anexos	20



1. Acerca de

El plan de recuperación de desastres de Servicios Informáticos se establece con el fin de mitigar los efectos que puedan generarse a causa de algún desastre natural o humano accidental o intencionado. Es decir, cualquier evento mayor que afecte el funcionamiento de los servicios informáticos del H. Ayuntamiento Municipal de Taxco de Alarcón, Guerrero, México.

2. Alcance

El presente documento aplica a cualquier servicio informático que pueda verse afectado en caso de desastre. El plan de recuperación de desastres informáticos está construido para la ejecución de acciones preventivas y de control de emergencias, así como asegurar la continuidad de las operaciones de dichos sistemas en el menor tiempo posible, para esto se manejan las siguientes medidas:

- **Preventivas:** Identifica los riesgos y se establecen un conjunto de controles y acciones para solventar de manera oportuna cualquier eventualidad.
- **Organizativa y de respuesta:** Los sistemas de alerta, los planes de recuperación y los insumos requeridos para una respuesta rápida y eficiente en caso de contingencia.
- **Recuperación:** Acciones requeridas para la continuidad de la operación con el fin de que se restituyan las condiciones normales de trabajo en el menor tiempo posible.

3. Objetivos

3.1 Objetivo General

Asegurar la continuidad de los servicios informáticos del H. Ayuntamiento Municipal de Taxco de Alarcón a través de un conjunto de procedimientos que permitan responder en el menor tiempo posible y de manera adecuada desde el momento en que exista un fenómeno que pueda considerarse como desastre, hasta que se vuelva a la normalidad.

3.2 Objetivos Específicos

1. Prevenir cualquier situación que pueda afectar a los servicios informáticos esenciales para el funcionamiento del H. Ayuntamiento Municipal de Taxco de Alarcón, así como establecer medidas para solventar de manera eficiente dichas funciones.
2. Disminuir la magnitud de cualquier pérdida mediante la reducción del tiempo de la interrupción de los servicios informáticos.
3. Identificar los daños, los procedimientos para repararlos y ejecutar las acciones requeridas para la recuperación de las actividades.
4. Evitar la pérdida de datos de sistemas informáticos imprescindibles para la operación de del H. Ayuntamiento Municipal de Taxco, y en caso de ocurrir asegurar la recuperación de los mismos en el menor tiempo posible.
5. Preparar al personal de la dirección de Informática para responder con eficacia ante una situación de desastre y actuar sobre el proceso de recuperación.

4. Equipo De Recuperación

El equipo de recuperación está conformado por el personal de la dirección de informática. Estas personas serán las encargadas de llevar a cabo el Plan De Recuperación De Desastres, cada individuo tiene funciones a desarrollar según su rol. Los integrantes del equipo y sus funciones durante una situación de emergencia se muestran en la tabla a continuación:

EQUIPO DE RECUPERACIÓN DE DESASTRES

Director de Informática	Encargado de dirigir las acciones durante la contingencia. Responsable de tomar las decisiones importantes durante alguna situación de crisis. Es el principal responsable de coordinar a los miembros de equipo. Realiza labores de reparación de hardware y software de manera activa para verificar y mejorar la coordinación entre ambos indoles. Responsable de investigar, experimentar diferentes formas de mitigar el desastre en caso de que lo estipulado en este manual no funcione de manera adecuada o la situación sea diferente a como fue planteada.
Subdirector de Informática	Ayuda en la coordinación de acciones y en la toma de decisiones. Segundo responsable de investigar, experimentar y sugerir al director diferentes formas de mitigar el desastre en caso de que lo estipulado en este manual no funcione de manera adecuada o la situación sea diferente a como fue planteada. Responsable de efectuar las decisiones tomadas por el director en el ámbito del software, como lo es la recuperación de archivos en discos duros, eliminación de virus informáticos, configuración de equipos de red para su funcionamiento, etc.
Subdirector de Soporte Técnico	Responsable de efectuar las decisiones tomadas por el director en el ámbito del hardware, como lo es la instalación física de equipos de red, de cómputo, la instalación de cableado, etc. Participa en la configuración de estos equipos.
Auxiliar técnico	Ayuda en la ejecución de las labores de hardware y de software según se le necesite con más urgencia.

5. Procedimientos De Recuperación

A continuación, se muestran las acciones detalladas que se deben realizar para mantener la continuidad de las operaciones en caso de una situación que pueda ser considerada como desastre; ya sea de origen natural, causada por el hombre o de origen tecnológico, con la intención de mantener las operaciones esenciales del H. Ayuntamiento Municipal de Taxco de Alarcón.

5.1 Acciones preventivas para situación de desastres

Para prevenir los desastres se han establecido una serie de acciones con la finalidad de tener las herramientas necesarias y de esta manera garantizar las acciones pertinentes durante algún desastre, reduciendo la pérdida de información y garantizando el restablecimiento de los servicios informáticos en el menor tiempo posible.

5.1.1 Del servidor web y de correos

El servidor web y de correos se encuentran en el mismo servidor. Es un servicio que es arrendado en la compañía de nombre "GoDaddy". La empresa tiene su sede central la ciudad de Tempe en la ciudad de Arizona en Estados Unidos.

Este servidor contiene la información de la página web del H. Ayuntamiento Municipal de Taxco de Alarcón; en la cual se muestran noticias, próximos eventos y convocatorias dentro del municipio, parte del portal de transparencia, entre otras secciones habidas y por haber y, también, las direcciones de correo institucional junto a sus mensajes enviados y recibidos.

Desde mediados de marzo del 2022, fecha de comienzo de la renta de este servicio, el respaldo de la información se hace de manera diaria y de manera automática. Gracias al plan de renta que se tiene desde tales fechas, en caso de contingencia, se puede acceder y restaurar esta copia de seguridad de antigüedad de un día anterior. En otras palabras, en caso de que un incidente ocurriera un día viernes, es posible restaurar la copia de seguridad del día jueves, teniendo como rezago la información creada y modificada el día de la crisis, el día viernes.

Para evitar situaciones que afecten el funcionamiento de los correos electrónicos donde se vea comprometidos la dirección de correo o la información de las personas que estos los utilizan (Por ejemplo, el Phishing o descargas de algún malware, spyware, ransomware, etc.). Se tienen activos:

- **Filtros contra spam activos:** 633 filtros.
- **Filtros de correo electrónico:** 30 sentencias (Es un filtro el cual de manera automática lee todos y cada uno de los mensajes que llegan a todas las direcciones de correo electrónico y mediante varias configuraciones este evalúa si el mensaje debe ser eliminado o no).
- **Direcciones IP Bloqueadas:** 17 IPs individuales y 1 rango de IP (51.0.0.0/8).

Los filtros mencionados están en constante actualización por parte de la dirección de informática de manera diaria, se verifica su correcto funcionamiento y se afina el filtrado de los mensajes. En caso de que todos los filtros fallen, se ha hecho saber a todas las áreas del H. Ayuntamiento Municipal que en caso de la más mínima duda de la veracidad de un correo electrónico se llame de manera inmediata a cualquier miembro de la dirección de informática para que se verifique la autenticidad. Esto se hace mediante la lectura de los "encabezados del mensaje", donde se puede observar el verdadero lugar de origen del mensaje, además de, por supuesto, la lectura del mensaje y la verificación de los archivos y links que en él se contienen.

5.1.2 De las computadoras pertenecientes al H. Ayuntamiento Municipal

Para mantener respaldada la información de los equipos de cómputo, los integrantes de la dirección de informática deberán extraer uno a uno los equipos de cómputo de las diferentes áreas prioritarias del H. Ayuntamiento Municipal de Taxco de Alarcón para posteriormente realizar un copiado de los archivos que en estas computadoras se contiene.

La información se almacenará en primera instancia en un par de discos duros externos, posteriormente, la información pasará a ser almacenada en una nube local que está configurada en modo espejo; es decir, la nube tiene dos discos duros de gran capacidad de almacenamiento, la información se guarda en los discos al mismo tiempo, así en caso de que un disco falle el otro seguirá conteniendo la información intacta. Este proceso se realizará cada 2 meses y se le notificará al área de uno a dos días hábiles antes para que preste las facilidades de retirar momentáneamente los equipos de cómputo uno a uno que al área pertenezcan.

Las áreas consideradas como prioritarias son las que a continuación se enlistan en orden alfabético:

- Oficialía Mayor
- Presidencia Municipal
- Secretaría de Obras Públicas y Ramo XXXIII
- Secretaría General
- Sindicatura
- Tesorería

En caso de que la información del equipo de cómputo a respaldar se considere confidencial o de carácter sensible se omitirá el respaldo de esta por parte de la dirección de Informática, sin embargo, se le exhortara al área en cuestión que haga su propio respaldo para evitar la pérdida de información por factores naturales, humanos o tecnológicos.

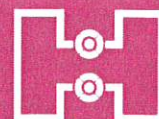
5.1.3 De la red de telecomunicaciones

La red de telecomunicaciones es el espacio por donde la información de las computadoras, impresoras, teléfonos celulares, etc. viaja interconectando artefactos entre sí y en entre diferentes sistemas de manera alámbrica y/o inalámbrica ya sea de manea local (geográficamente hablando) o de manera externa (hacia la internet).

Desde el primer día de labores de este gobierno la red sufrió bastantes modificaciones con el fin de mejorar el ancho de banda y la latencia de los datos. Se reemplazaron y eliminaron los equipos de red y el cableado obsoleto y averiado siendo reemplazados por materiales y artefactos de mejor calidad. Aun hacen falta lugares donde se puede mejorar la red, sin embargo, los lugares críticos ya fueron restaurados como lo fue tesorería, obras públicas, oficialía y catastro.

Para evitar averías en esta red se ha hecho la estructuración de cable lo más alta posible, es decir, se ha engrapado (con grapas curvas) el cable a la altura más alta posible según las condiciones del entorno lo permitan. Con ellos se evita que el cable se averíe por pisotones o jalones, además de que se ha evitado el pasar el cable por lugares donde pueda ser dañado fácilmente, por ejemplo, en paredes con humedad o calor excesivo. Aunado a lo anterior, se han retirado los equipos de red que no son necesarios en la infraestructura de la red, quitando así 'saltos' innecesarios dentro de la red, disminuyendo así la latencia de la información que viaja hacia la internet.

Es de reconocer que la red aún no está en su en su mejor estado debido principalmente lo caro que puede llegar a ser el material para redes (cables, conectores, herramientas, switches, routers, etc.) la red podría ser mucho mejor. Sin embargo, ya se está trabajando en un proyecto para hacer mucho más eficiente esta red de comunicación y mejor la comunicación entre equipos y hacia la internet.



5.1.4 Del Sistema SUINPAC

Las acciones preventivas tomadas por el sistema SUINPAC se anexan al final en forma de copia fotostática.

5.2 Acciones organizativas y de respuesta

En caso de contingencia en alguno de los servicios informáticos o sobre la infraestructura misma, se tienen como pasos a seguir los que a continuación se describen en los diversos puntos que se plasma en este documento.

5.2.1 Contingencia en el servidor web y de correos

- **Caída momentánea del servidor (Contingencia menor):** Es común que los servidores web, de correo o de cualquier otro servicio sufran lapsos de desconexión. Muchas veces no es el servidor en si el que sufre algún altercado, sino parte de la infraestructura que se debe tomar para llegar hacia él. Razón por la cual se le considera como un incidente menor.

Sin embargo, la dirección de Informática no se da el lujo de quedarse con las manos cruzadas esperando a que el problema se solucione. Si bien no hay manera de que los integrantes de dicha área intervengan de manera directa, se debe de reportar vía telefónica o por mensajería de WhatsApp la caída a la empresa arrendadora (GoDaddy) para que ella tome cartas en el asunto y verifique si ha sido el servidor el que está teniendo el problema o se debe a una falla en la infraestructura de la internet; lo último puede sonar descabellado, pero es más común de lo que parece.

La tarea de reportar las fallas en el servidor generalmente es llevada a cabo por el director del área, el subdirector de informática o en su defecto por el auxiliar técnico.

- **Problemas en la recepción y envío de correos electrónicos (Contingencia media):** En caso de que la recepción y/o envío de correos se vea afectada haciendo que los mails generados por alguno de los correos institucionales no estén siendo recibido por el o los otros extremos del canal de comunicación, se deberán tomar las siguientes acciones:
 1. Reportar vía telefónica o por WhatsApp a GoDaddy el problema del servicio.
 2. Revisar en la configuración del servidor que los registros de DNS apunten a las direcciones correctas, caso contrario editar los registros con los datos apropiados.
 3. Si el problema persiste por más de 5 minutos se le hará de conocimiento de manera verbal a las áreas del H. Ayuntamiento Municipal el problema para que utilicen alternativas (Correos electrónicos alternativos) para comunicarse con quien sea necesario para cambiar de manera momentánea el canal de comunicación y tratar de no perjudicar ni detener el intercambio de información en el tiempo en que el problema se soluciona.
 4. Se verificará que en el servidor de nombres ("AKKY") el nombre de dominio este apuntando de manera correcta a los servidores de GoDaddy.
 5. Una vez el servicio se haya reestablecido, se hará reporte de la situación a Oficialía Mayor por medio de un oficio donde se indiquen las posibles causas y los efectos que el problema ha provocado; como correos perdidos o que no pudieron ser enviados.

La tarea de reportar y reparar las fallas en la recepción y envío de correos generalmente es llevada a cabo por el director del área, el subdirector de informática o en su defecto por el auxiliar técnico.

- **Inaccesibilidad a cualquiera de los servicios del servidor por un lapso prolongado (Contingencia crítica):** En caso de que el sistema de correos se vea inutilizable y/o la página web sea inaccesible en un lapso mayor o igual a 10 minutos, las acciones a tomar serán las siguientes:

1. Reportar vía telefónica o por medio de WhatsApp, de manera inmediata, el problema a la empresa arrendadora GoDaddy, en caso de que aún no se haya hecho. Si ya ha sido reportado el problema, se deberá de insistir en la resolución del problema. Al ser una empresa internacional, la lista de espera para ser atendido puede ser de un par de minutos hasta horas, de ahí la importancia en insistir por los diferentes medios de comunicación para ser atendido.
2. Se le hará de conocimiento de manera verbal a las áreas del H. Ayuntamiento Municipal el problema para que utilicen alternativas (Correos electrónicos alternativos) para comunicarse con quien sea necesario para cambiar de manera momentánea el canal de comunicación y tratar de no perjudicar ni detener el intercambio de información en el tiempo en que el problema se soluciona.
3. Se verificará que en el servidor de nombres ("AKKY") el nombre de dominio este apuntando de manera correcta a los servidores de GoDaddy.
4. Se hará investigación sobre algunas caídas dentro de los servicios de algún DNS de la internet que puedan estar perjudicando al servidor perteneciente al ayuntamiento; por ejemplo, caídas en los servidores de Cloudflare (1.1.1.1). De ser así, se le hará de conocimiento a la persona que esté atendiendo el problema técnico. Toda la información técnica que pueda ser útil es buena que sea proporcionada a servicio de asistencia técnica de GoDaddy.
5. Una vez el servicio se haya reestablecido, se hará reporte de la situación a Oficialía Mayor por medio de un oficio donde se indiquen las posibles causas y los efectos que el problema ha provocado; como correos perdidos o que no pudieron ser enviados.

5.2.2 Contingencia en alguna computadora del H. Ayuntamiento Municipal

En caso de contingencia en una o varias computadoras pertenecientes a este ayuntamiento, se tienen como pasos a seguir lo siguiente:

- **Por pérdida de información por eliminación (Contingencia Media):** Es normal cometer errores. A veces esos errores pueden provocar que de manera accidental (o también intencionada) que parte o toda la información de una computadora se pierda (Documentos, imágenes, videos, etc.). Así que, en caso de que sucede algo de este estilo, se deberá hacer lo siguiente:

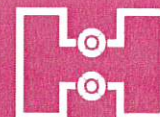
1. Extraer la o las computadoras que perdieron información
2. Retirar momentáneamente el o los discos duros que cada computadora contenga
3. Se verificará que la falla no haya sido por algún mal funcionamiento del hardware, esto mediante una observación a fondo de la parte física externa del disco duro.
4. El disco duro se conectará mediante un adaptador de discos duros SATA a USB a alguna computadora perteneciente a la dirección de informática o de sus integrantes y se verificará su salud con el software *CrystalDiskInfo*.
5. Se comenzará con la recuperación de archivos los softwares *Hetman* y *Recuva*.
6. Los archivos serán puestos de nueva cuenta en el disco duro anteriormente afectado y esta pieza será nuevamente instalada en la computadora para después ser entregada a su área correspondiente.

NOTA IMPORTANTE: También puede ser reestablecido un respaldo de los archivos, si es que se cuenta con el en la dirección de informática y que no tenga una antigüedad tan extensa donde pueda afectar las actividades del área. Es decir, si los archivos perdidos están en constante actualización es preferible intentar recuperarlos antes de restaurar una copia de seguridad, puesto que puede afectar de mala forma la continuidad de la información.

- **Por pérdida de información provocada por falla en el sistema operativo (Contingencia Leve):** Suele suceder, mayormente a causa de apagones repentinos en las computadoras, que los sistemas operativos se dañen, dejando así inaccesible la información que se almacena en la computadora afectada:
 1. Tomar la computadora afectada a las oficinas de Informática
 2. Con ayuda de una USB “booteada” con alguna distribución Linux (Preferentemente alguna distro que no consuma muchos recursos como ‘Zorin Os’) se inicializará la computadora.
 3. Se conectará a la computadora un disco duro, cuyo propósito es el respaldar archivos rescatados y por medio del uso del ya mencionado sistema operativo almacenado en la USB se comenzará a respaldar la información de un disco a otro.
 4. Terminado el proceso, al disco duro perteneciente a la computadora afectada se le reinstalará el sistema operativo Windows (Puede ser en su versión Windows 10 o 7, dependerá de las prestaciones del equipo).
 5. Se le instalarán los programas necesarios para el desarrollo de las labores. Paquetería de Office, Adobe Reader, etc.
 6. Se trasladarán los archivos rescatados al disco duro que antes estaba afectado. Y la computadora se entregará al área que pertenece.

NOTA: Se hace de esta manera debido a que una gran mayoría de las computadoras pertenecientes a este ayuntamiento tienen contraseña de acceso. Provocando que, si se conectara directamente el disco duro a una computadora, este no pueda ser leído en su totalidad pues solicitará una clave de acceso. Con el uso de un sistema operativo Linux (O simplemente que no sea alguna versión Windows) se podrá evitar ese filtro de seguridad que se tiene.

NOTA II: Si la información del disco duro está encriptada, será imposible rescatar información de este disco duro.



- **Por pérdida de información provocada por virus (Contingencia Media):** Para solucionar este problema se deberán seguir los siguientes pasos:
 1. Extraer la computadora de su área y llevarla a las oficinas de la Dirección de Informática.
 2. Evaluar la situación, revisar que tipo de virus es y que afectaciones está provocando en equipo de cómputo.
 3. Según los resultados del análisis, utilizar las herramientas adecuadas para la eliminación del virus, por ejemplo, KVRT, Kaspersky antivirus, herramientas de análisis de Malware en línea, etc.
 4. En caso de que haya información dañada o eliminada se pueden utilizar programas como *Hetman* y *Recuva*.
 5. Una vez reparada la computadora, se deberá entregar a su respectiva área.

NOTA: En determinados casos, existen virus que por su reciente creación aún no hay cura o por su forma de actuar llegan a ser muy difíciles o simplemente imposibles de eliminar para rescatar la información, por ejemplo, el Ransomware de nombre WannaCry, el cual encripta la información. La computadora puede ser rescatada, pero no los datos.

- **Por pérdida de información provocada por falla en el hardware (Contingencia Mayor):**

Cuando existe este tipo de problemática se deberá proceder a realizar los siguientes pasos con extremo cuidado para no dañar de más el hardware afectado:

1. Extraer la computadora del área y llevarla a las oficinas de informática.
2. Abrir el equipo de computo y sacar el disco duro para posteriormente verificarlo visualmente a detalle y tratar de encontrar algún indicio de daño (Por caídas, por golpes, etc.)
3. Conectar el disco duro a alguna computadora mediante un adaptador y verificar su saludo con *CrystalDiskInfo*.
4. En caso de que el disco duro no se detecte, se deberán realizar maniobras mucho más avanzadas. Para como mínimo intentar una lectura de dicha pieza.
5. Puede suceder que se escuche un pequeño ruido o se sienta una especie de vibración en el disco duro (Solo si es de tipo mecánico). De ser así no se podrá hacer nada debido a que los componentes internos del disco estarán totalmente estropeados.
6. Si la situación lo permite o amerita, se pueden sustituir las piezas exteriores del disco duro.
7. Una vez reparado el disco duro, se regresará el disco duro instalado y la computadora al área a la cual pertenece.

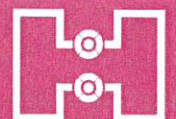
5.2.3 Contingencia en la red de telecomunicaciones

- **Por falla en algún cable (Contingencia Leve):** Comúnmente, los cables pueden llegar a dañarse ya sea por pisotones, dobleces de más de 90 grados, por la exposición prolongada al sol o simplemente por que el cobre y el plástico que componen a este medio se vuelven viejos. Es por ello que, cuando se deba reemplazar uno de estos cables se deberá hacer lo siguiente:

1. Identificar el cable dañando.
2. Comprobar que los extremos, en la parte del RJ45 están bien ponchados.
3. Si el este fue dañado en alguno de los extremos por algún mal dobles, se deberá verificar si la parte afectada puede ser cortada sin mayor problema, de ser así se retirará y se reponchará el extremo y se reconectará a donde corresponde.
4. En caso de que el cable no pueda ser reparado en el paso anterior, se deberá sustituir completamente.

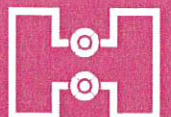
NOTA: La red inalámbrica también puede tener fallas. Por la naturaleza del entorno de Casa Janna y de Presidencia las antenas pueden presentar desperfectos en la transmisión de datos si es que la antena y el equipo de cómputo están separados por una pared de piedra o adobe. Es por ello que siempre se han conectado todas las computadoras hacia un cable de red. Es preferible que sea así, en especial en áreas recaudadoras. Esto para no presentar malfuncionamientos al momento de registrar datos en el sistema de SUINPAC. En caso de presentar fallas la antena, simplemente se desconectará de la corriente eléctrica por un par de minutos.

- **Por falla en algún nodo de red (Contingencia Media):** En caso de que algún nodo de red, como switches o routers fallen, se deberá hacer lo siguiente:
 1. Ubicar el nodo de red con fallas.
 2. Revisar que todos los cables estén conectados de manera correcta, de esta manera se descarta que el mal funcionamiento sea debido una mala conexión de un cable.
 3. Si no se soluciona el problema con el anterior paso, se deberá desconectar el aparato de la corriente eléctrica por lo menos 1 minuto, para posteriormente reconectarlo.
 4. Si después de 5 minutos el problema no se resuelve, el aparato deberá ser reiniciado de fabrica y posteriormente se le deberá meter el backup de su configuración (Este paso solo aplica para dispositivos administrables).
 5. En determinado caso que el problema siga sin solucionarse, el aparato deberá ser sustituido por alguno que este dentro de la reserva de informática. En caso de ser administrable se le deberá insertar la misma configuración
 6. Posteriormente, el aparato defectuoso deberá ser revisado a detalle en búsqueda de alguna falla en el hardware o software. Si es reparado se devolverá al lugar donde pertenece, de lo contrario será almacenado para su posterior baja.



- **Por falla en los puertos de red del dispositivo (Contingencia Media):** Los puertos de un dispositivo de red se pueden dañar por su uso prolongado o por algún mal movimiento, en caso de suceder lo anterior se deberá hacer lo siguiente:
 1. Localizar el puerto de red dañado.
 2. Desconectar el cable que está conectado sobre ese puerto.
 3. El cable ahora desconectado se conectará a otro puerto que sí funcione
 4. En caso de que el dispositivo de red sea administrable, se deberá configurara el puerto anteriormente mencionado según sea el caso y las necesidades.

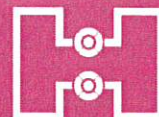
- **Por falla en los servicios de ISP Telmex (Contingencia Mayor):** No muy a menudo el servicio de internet de Telmex presenta malfuncionamiento. A menudo es porque esta empresa le da mantenimiento a su infraestructura, aunque también puede suceder por la caída de un poste o por el corte en alguna de las líneas de datos principales, de todo esto el resultado siempre será que no habrá internet. Si algo de eso llega a suceder, se deberá realizar lo siguiente:
 1. Llamar a la línea de asistencia de Telmex y reportar el problema. Se debe de insistir y hacer énfasis en la importancia de la recuperación del servicio debido a que sin internet el ayuntamiento prácticamente no podrá utilizar el sistema de SUINPAC, imposibilitando muchas tareas como lo es el cobro de algunos trámites.
 2. Solo en dado caso de que por lo menos uno de los módems sí funciones, de manera inmediata se canalizará la señal de internet solo a áreas prioritarias como lo es Tesorería, Cajas de Cobro, Dirección de Licencias y Permisos, Catastro, Predial, Registro Civil, Oficialía, Presidencia y Sindicatura. Lugares donde la señal de internet sea vital para realizar las labores del día a día. Esto se hará mediante movimientos en el cableado y algunas configuraciones para evitar que la escasa señal de internet sea utilizada para temas ajenos a los laborales; como ver videos en YouTube.





5.2.4 Contingencia en el sistema SUINPAC

Las acciones en caso de alguna contingencia tomadas por el sistema SUINPAC se anexan al final en forma de copia fotostática.



6. Anexos

A partir de la siguiente página se anexan los documentos que en la siguiente tabla se enlistan:

#	DOCUMENTOS
1	Plan de Recuperación de Desastres del Sistema SUINPAC



Plan de Recuperación en caso de desastres

SUINPAC.COM

Chilpancingo de los Bravo, Guerrero a 01 de enero de 2022.

Este plan de Recuperación de desastres está diseñado para asegurar la continuidad de los servicios técnicos del sistema SUINPAC. (fallas eléctricas, sismos, incendios).

Objetivos:

- Evitar o limitar la pérdida de información, servicios informáticos, y aplicaciones.
- Evitar daños en la infraestructura tecnológica.
- Recuperación de la información vital para el funcionamiento del sistema.
- Capacitar al personal de tecnologías para actuar en caso de desastres.

Procedimientos:

1. Revisar la magnitud del problema.
2. Desconectar el equipo electrónico (servidores, servidores de red, firewalls, etc.) del site, y de las áreas de oficinas.
3. Revisar la red eléctrica de manera general.

Detallado de fallas específicas:

Falla en Energía Eléctrica y Conexión de internet

Se considera Falla de energía eléctrica a partir de 12 horas, debido a que actualmente se cuenta con planta de energía de reserva con duración aproximada de 12 horas, terminado el tiempo, es necesario rellenar el depósito de combustible para mantener en funcionamiento el servidor.

Con respecto a la conexión de internet, actualmente contamos con 2 líneas de internet de diferentes compañías, para mantener el servicio del sistema al exterior, en caso de que la conexión principal falle, en automático la conexión de respaldo entra en funcionamiento, esto gracias a la configuración establecida en el servidor de red.

En caso de que las 2 líneas de internet fallen, el servicio se proporciona por medio de internet satelital, a un ancho de banda mínimo.

Sismos

México es una zona sísmica, por lo cual se considera lo siguiente:

Revisión de la infraestructura de red y eléctrica.

Revisión del equipo electrónico (servidores, servidores de red, firewalls, etc.) del site, y de las áreas de oficinas.

Incendio

Los incendios Son considerados situaciones de emergencia frecuente en el ambiente laboral.

Posterior al incendio, proceder a la revisión de la infraestructura de red y eléctrica.

Revisión del equipo electrónico (servidores, servidores de red, firewalls, etc.) del site, y de las áreas de oficinas.

Plan de Respaldo

1. Respaldo de las bases de datos diario, manteniendo 1 respaldo diario de los últimos 30 días, posterior a esto, solo se mantiene 1 respaldo mensual hasta llegar a 12 respaldos para no sobrecargar las unidades de almacenamiento. Posterior a esto se van eliminando los respaldos más antiguos.
2. Respaldo del código fuente y aplicaciones diario, estos respaldos siguen la misma regla del respaldo de la base de datos.
3. Adicionalmente, se sube a un servidor privado en la nube, 1 respaldo diario de base de datos y código y solo se mantienen durante 7 días. Después de esto se van eliminando los más antiguos.

	Elaboró	Revisó	Autorizó
Area	Desarrollo Tecnológico	Dirección Administrativa	Dirección General
Nombre	Ing. Erik Francisco Valle Camacho	C.P. Alfredo Escobar Corona	C.P. Said Pineda Arroyo