Plan de Contingencias para Respaldo de Información de Equipo y Sistemas Informáticos

Unidad de Gestión de la Calidad e Informática

Sistema para el Desarrollo Integral de la Familia de Baja California (DIF BC)

Mexicali, Baja California, Julio de 2025

Página de Publicación:

https://www.difbc.gob.mx

ÍNDICE

1. Introducción

2. Objetivo

   2.1 Objetivo General

   2.2 Objetivos Específicos

3. Alcance

4. Identificación de Procesos y Servicios

   4.1 Procesos de Software Identificados

   4.2 Servicios Críticos a Restablecer

   4.3 Software Base

   4.4 Respaldo de la Información

5. Análisis de Evaluación de Riesgos y Estrategias

   5.1 Metodología Aplicada

   5.2 Clasificación de Riesgos

   5.3 Clases de Riesgos y Acciones Correctivas

      5.3.1 Incendio o Fuego

      5.3.2 Robo de Equipos y Archivos

      5.3.3 Fallas en los Equipos

      5.3.4 Errores en el Manejo del Sistema

      5.3.5 Virus Informáticos

      5.3.6 Fenómenos Naturales

      5.3.7 Accesos No Autorizados

      5.3.8 Fallas de Red

6. Eventos Considerados en el Plan de Contingencias

6.1 Falta de Comunicación entre Usuario y Servidor

6.2 Fallas del Equipo Servidor

6.2.1 Error Físico de Disco

6.2.2 Error de Memoria RAM

6.2.3 Fallas en la Tarjeta Madre u Otro Componente Interno

6.2.4 Error Lógico de Datos

6.2.5 Acciones en Caso de Fallas Críticas

6.2.6 Acciones en Caso de Vulneración o Hackeo

7. Plan de Recuperación y Respaldo de la Información

7.1 Procedimientos Documentados en SICADIF

7.2 Clasificación del Plan de Recuperación

7.2.1 Actividades Previas al Desastre

7.2.2 Actividades Durante el Desastre (Plan de Emergencias)

7.2.3 Actividades Posteriores al Desastre

8. Conclusiones

9. Recomendaciones

1. INTRODUCCIÓN

El presente **Plan de Contingencias** para el Respaldo de Información Equipo y Sistemas Informáticos de la Unidad de Gestión de la Calidad e Informática del Sistema para el Desarrollo Integral de la Familia de Baja California, podemos definirlo como el **conjunto de procedimientos alternativos a la operatividad normal de la institución, cuya finalidad es la de permitir el funcionamiento de ésta, aun cuando alguna de sus funciones deje de hacerlo debido a algún incidente, desastre o sabotaje tanto interno como ajeno a la Institución.** Las causas son variadas y pasan desde un problema informático, un fallo en energía eléctrica, telecomunicaciones, hasta desastres naturales o sabotajes.

El Plan de Contingencias no implica un reconocimiento de la ineficiencia, supone un importante avance a la hora de superar todas aquellas situaciones descritas anteriormente que pueden provocar importantes pérdidas, no sólo materiales sino de la información, así también como de aquellas derivadas de la paralización de las funciones de la institución durante un periodo de tiempo determinado. El presente documento pretende ayudar a comprender mejor la problemática del entorno informático, ya que toda la institución debe estar preparada para el caso de ocurrencias imprevistas.

Para su elaboración se contó con la participación del personal de la Unidad de Gestión de la Calidad e Informática y la autorización de la Titular de la Dependencia.

Los trabajos de coordinación para la actualización de este documento se realizarán de forma anual por la Unidad de Gestión de la Calidad e Informática, así también, cuando las necesidades de la Institución lo requieran (o lo demanden).

2. OBJETIVO

2.1 Objetivo General

El **principal objetivo** de un Plan de Contingencias de la Unidad de Gestión de la Calidad e Informática es la de g**arantizar la continuidad de las operaciones dentro de la institución, a fin de que se restablezcan en el menor tiempo posible, en caso de la**

ocurrencia de alguna eventualidad que interrumpa su funcionamiento.

2.2 Objetivos Específicos

- *Minimizar el tiempo de inactividad.*
- *Restaurar datos críticos y servicios esenciales.*
- *Reducir el impacto económico y operativo.*
- *Establecer roles y responsabilidades claras.*
- *Asegurar la continuidad de las operaciones dentro de la institución.*

3. ALCANCE

Están comprendidos en la ejecución del presente Plan, los directivos, personal encargado del equipo de informática y los responsables de cada área de las oficinas de la Unidad de Gestión de la Calidad e Informática.

4. IDENTIFICACIÓN DE PROCESOS Y SERVICIOS

- *Principales Procesos de Software Identificados:*
- *Nómina*
- *Contabilidad*
- *Presupuestos*
- *Padrones de información de beneficiarios*
- *Sistemas de Procuraduría*
- *Gestión Documental*
- *Página institucional*
- *Servicios Web de aplicaciones móviles*
- *Principales servicios que deberán ser restablecidos y/o recuperados*
- *Correo Electrónico.*
- *Internet.*
- *Portales de sitios Web.*
- *Antivirus.*
- *Herramientas de Microsoft Office.*
- *Telefonía.*
- *Energía eléctrica.*
- *Software Base*

- *Base de Datos.*
- *Respaldo de la Información.*
- *Ejecutables de las aplicaciones.*
- *Respaldo de la Información*
- *Respaldo de la Base de Datos.*
- *Respaldo de la Plataforma de Aplicaciones (Sistemas).*
- *Respaldo de Sitios WEB.*
- *Respaldo de correo electrónico*
- *Respaldos de discos duros compartidos*

5. ANÁLISIS DE EVALUACIÓN DE RIESGOS Y ESTRATEGIAS

5.1 Metodología aplicada

Para la **Clasificación de los activos de las Tecnologías de Información de la Unidad de Gestión de la Calidad e Informática** se han considerado tres criterios:

1. **Grado de negatividad:** Un evento se define con grado de negatividad (Leve, moderada, grave y muy severo).
2. **Frecuencia del Evento:** Puede ser (Nunca, aleatoria, periódico y continuo)
3. **Impacto:** El impacto de un evento puede ser (Leve, moderado, grave y muy severo).

Plan de Contingencia

Son procedimientos que se definieron en la institución pretenden continuar o recuperar las funciones críticas en caso de una interrupción no planeada.

Los sistemas son vulnerables a diversas interrupciones, que se pueden clasificar en:

- ***Leves*** *(Caídas de energía de corta duración, fallas en disco duro, etc.)*
- ***Severas*** *(Destrucción de equipos, incendios, etc.)*

5.2 Clasificación de riesgo

La vulnerabilidad de los activos o bienes, ante un posible o potencial perjuicio o daño. Se clasificaron en:

- ***Riesgos Naturales***: tales como mal tiempo, lluvia en exceso, huracanes, terremotos, etc
- ***Riesgos Tecnológicos:*** tales como incendios eléctricos, fallas de energía y accidentes de transmisión o transporte.
- ***Riesgos Sociales:*** bloqueo de acceso a instalaciones.

Los elementos de riesgos a los cuales está expuesto el conjunto de equipos informáticos y la información procesada de la institución se describe a continuación.

Activos susceptibles de daño

- *Personal*
- *Hardware*
- *Software y utilerías*
- *Datos e información*
- *Documentación*
- *Suministro de energía eléctrica*
- *Suministro de telecomunicaciones*
- *Posibles daños*

Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas.

Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.

Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante Robo o Incidencia.

Fuentes de daño

- *Acceso no autorizado.*
- *Ruptura de las claves de acceso a los sistemas computacionales.*
- *Desastres Naturales (Movimientos telúricos, Inundaciones, Fallas en los equipos de soporte causadas por el ambiente, la red de energía eléctrica o el no acondicionamiento*

atmosférico necesario, caída o desajuste de antenas por viento).

- *Faltas de Personal Clave (Enfermedad, Accidentes, Renuncias, Abandono de sus puestos de trabajo, entre otros).*
- *Fallas de Hardware (Falla en los Servidores o falla en el hardware de Red (Switches), cableado de la Red, Router, Firewall).*

5.3 Clases de Riesgos y acciones correctivas

- *Incendio o Fuego*
- *Robo común de equipos y archivos*
- *Falla en los equipos*
- *Acción virus informático*
- *Fenómenos naturales*
- *Accesos no autorizados*
- *Ausencia del personal de sistemas.*
- *Uso malintencionado o desinformado de equipo de cómputo o de sistemas de información.*

Minimizar el riesgo

Teniendo en cuenta lo anterior, corresponde al presente Plan de Contingencias minimizar estos índices con medidas preventivas y correctivas sobre cada caso de Riesgo. Es de tener en cuenta que en lo que respecta a fenómenos naturales, las que podrían producir daños estructúrales en los edificios.

5.3.1 Incendio o Fuego

- ***Grado de Negatividad:*** *Muy Severo*
- ***Frecuencia de Evento:*** *Aleatorio*
- ***Grado de Impacto:*** *Alto*

Analizando el riesgo de incendio, se permite resaltar el tema sobre el lugar donde almacenar los respaldos.

El incendio, a través de su acción calorífica, es más que suficiente para destruir los dispositivos de almacenamiento, al como DVD y Discos duros.

Uno de los dispositivos más usados para contrarrestar la contingencia de incendio, son los extinguidores. Su uso conlleva

a colocarlos cerca de las posibles áreas de riesgo que se debe proteger.

Con la instalación del sistema de detección, control y sofocación contra incendios, se tiene una mayor seguridad de poder contrarrestar cualquier situación que se presente con un incidente de este tipo.

5.3.2 Robo Común de Equipos y Archivos

- ***Grado de Negatividad:*** *Grave*
- ***Frecuencia de Evento:*** *Aleatorio*
- ***Grado de Impacto:*** *Moderado*

Es relativamente sencillo sustraer componentes de un CPU —como discos duros, lectoras, tarjetas u otros dispositivos— sin que el faltante sea detectado de manera inmediata, pudiendo transcurrir varios días antes de advertirse la pérdida.

Aunque estas situaciones no se han presentado en nuestra dependencia, se recomienda mantener en todo momento una actitud de alerta y vigilancia, con el fin de prevenir incidentes que comprometan los recursos tecnológicos de la institución.**IV.1.3**

5.3.3 Falla en los Equipos

- **Grado de Negatividad:** Grave
- **Frecuencia de Evento:** Aleatorio Grado
- **de Impacto:** Grave

Teniendo en cuenta la importancia del flujo eléctrico para el funcionamiento del área, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. El equipo de aire acondicionado y ambiente adecuado en el Área de Servidores favorece su correcto funcionamiento.

Para el adecuado funcionamiento de las computadoras personales de escritorio, necesitan de una fuente de alimentación eléctrica fiable, es decir, dentro de los parámetros correspondientes. Si se interrumpe inesperadamente la alimentación eléctrica o varía en forma significativa (fuera de los valores normales), las consecuencias pueden ser muy serias, tal como daño del Hardware y

la información podría perderse. La fuente de alimentación es un componente vital de los equipos de cómputo, y soportan la mayor parte de las anomalías del suministro eléctrico.

Por lo anterior se debe tener en cuenta lo siguiente:

Sistema de Tierra Física:

Se denomina así a la comunicación entre el circuito eléctrico y el suelo natural para dar seguridad a las personas protegiéndolas de los peligros procedentes de una ruptura del aislamiento eléctrico. Estas conexiones a tierra se hacen frecuentemente por medio de placas, varillas o tubos de cobre enterrados profundamente en tierra húmeda, con o sin agregados de ciertos componentes de carbón vegetal, sal o elementos químicos, según especificaciones técnicas indicadas para las instalaciones eléctricas siguiendo las Normas Oficiales Mexicanas.

En la práctica protege de contactos accidentales las partes de una instalación no destinada a estar bajo tensión y para disipar sobretensiones de origen atmosférico o industrial. La toma a tierra tiene las siguientes funciones principales:

Protege a las personas limitando la tensión que respecto a tierra puedan alcanzar las masas metálicas.

Protege a personas, equipos y materiales, asegurando la actuación de los dispositivos de protección como: pararrayos, descargadores eléctricos de líneas de energía o señal, así como interruptores diferenciales.

Facilita el paso a tierra de las corrientes de defecto y de las descargas de origen atmosférico u otro.

Extensiones eléctricas, Barras Multicontactos Eléctricos.

Los equipos de cómputo requieren de tomas de corriente eléctrica. Pocas oficinas se encuentran equipadas con las suficientes placas de pared. Dado que es necesario conectar además algún equipo que no es informático, es fácil ver que son muy necesarias las extensiones eléctricas múltiples. El uso de estas extensiones eléctricas debe ser controlado con cuidado. No solo para que no queden a la vista, sino también porque suponen un peligro

considerable para aquellos que tengan que pasar por encima. A parte del daño físico que puede provocar engancharse repentinamente con el cable, apaga de forma rápida un sistema completo.

Corriente eléctrica regulada.

Todo equipo de cómputo debe estar protegido con corriente eléctrica regulada para evitar que el sistema eléctrico público descargue un flujo de energía superior a los valores establecidos para los circuitos domésticos y comerciales, por tal motivo, se debe contar con Unidades de Sistema de Alimentación Eléctrica Ininterrumpida (UPS) para que se regulen los valores permitidos y evitar con ellos que los equipos electrónicos sufran algún desperfecto.

Planta de energía eléctrica de respaldo y sistemas de Alimentación Eléctrica Ininterrumpidas (UPS).

Los Equipos y sistemas que conforman la Infraestructura de Tecnológica de la Institución deben de contar con un sistema de energía alterno, como lo son las Plantas de Energía Eléctrica de respaldo, Planta Generadora de Energía y los Sistema de Alimentación Eléctrica Ininterrumpida (UPS) son fundamental para asegurar la continuidad de las operaciones, especialmente en situaciones donde el suministro eléctrico principal falla o es interrumpido

5.3.4 Errores en el manejo del sistema

- ***Grado de Negatividad:*** *Moderado*
- ***Frecuencia de Evento:*** *Periódico*
- ***Grado de Impacto:*** *Moderado*

5.3.5 Acción de Virus Informático

- ***Grado de Negatividad:*** *Muy Severo*
- ***Frecuencia de Evento:*** *Continuo*
- ***Grado de Impacto:*** *Grave*

Los Virus informáticos han evolucionado de tal manera que hoy en día todos conocemos la importancia de tener un programa Antivirus en el equipo de cómputo y aún más importante es su actualización.

Si tenemos un antivirus instalado, pero no lo hemos actualizado, seguramente será capaz de encontrar los virus que intenten entrar en nuestros sistemas, pero no será capaz de hacer nada con ellos, dado que esta información está contenida en las definiciones de virus. La actualización del patrón de definiciones de virus es vital y debe de hacerse como mínimo una vez a la semana. Otra de las piezas esenciales del Antivirus, el motor, también debe actualizarse regularmente dado que los nuevos virus requieren en muchos casos nuevos motores de escaneo para poder detectarlos, por lo que la actualización del motor también es tarea obligada.

5.3.6 Fenómenos Naturales

- ***Grado de Negatividad:*** *Grave*
- ***Frecuencia de Evento:*** *Aleatorio Grado*
- ***de Impacto:*** *Grave*

La previsión de desastres naturales sólo se puede hacer desde el punto de vista de minimizar los riesgos necesarios en el área de servidores, en la medida de no dejar objetos en posición tal que ante un movimiento telúrico pueda generar mediante su caída y/o destrucción la interrupción del proceso de operación normal. Además, desde el punto de vista de respaldo, se debe tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, dispositivos de almacenamiento, discos con información vital, todo ello como respaldo de aquellos que se encuentren aun en las instalaciones de la institución.

5.3.7 Accesos No Autorizados

- ***Grado de Negatividad:*** *Grave*
- ***Frecuencia de Evento:*** *Aleatorio Grado*
- ***de Impacto:*** *Grave*

5.3.8 Fallas de Red

- ***Grado de Negatividad:*** *Grave*
- ***Frecuencia de Evento:*** *Aleatorio*
- ***Grado de Impacto:*** *Grave*

6. EVENTOS CONSIDERADOS PARA EL PLAN DE CONTINGENCIAS

Cuando se efectúa un riesgo, este puede producir un Evento, por tanto, a continuación, se describen los eventos a considerar dentro del Plan de Contingencias.

6.1 Falta de comunicación entre Usuario y Servidor – Servidor en la Unidad de Gestión de la Calidad e Informática existe el servicio de soporte técnico 1, la cual se activa al realizar una llamada telefónica por parte del usuario afectado, o cuando el usuario levanta orden de servicio por medio del portal de soporte.

Requerimiento del usuario se atiende de acuerdo a lo documentado de los procesos de atención de usuarios de la Coordinación de Tecnologías de la Información y Comunicación, y de Soporte de la Coordinación de Sistemas de la información.

Recursos de Contingencia

Los documentados en los procesos de las Coordinación de Tecnologías de la Información y Comunicación, y de Soporte de la Coordinación de Sistemas de la información, en el Sistema de Gestión de la Calidad de DIF (SICADIF)

6.2 Falla del Equipo Servidor

Puede producir pérdida de hardware y software, pérdida del proceso automático de Backup y Restore e Interrupción de las operaciones. A continuación, se describen algunas causas del fallo en un Servidor:

6.2.1 Error Físico de Disco en un Servidor

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

- *Ubicar el disco dañado.*
- *Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a directores y jefes de área.*
- *Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.*
- *Dar de baja el sistema y apagar el equipo.*

- *Retirar el disco dañado y reponerlo con otro del mismo tipo, hacer partición lógica y darle formato con el sistema operativo que estaba operando.*
- *Restaurar el último respaldo en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.*
- *Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.*
- *Habilitar las entradas al sistema para los usuarios.*

6.2.2 Error de Memoria RAM

En este caso se dan los siguientes síntomas:

- *El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.*
- *Ante procesos mayores se congela el proceso.*
- *Arroja errores con mapas de direcciones hexadecimales.*

Es recomendable que el servidor cuente con memorias ECC (error correct checking), por tanto, si hubiese un error de paridad, el servidor se autocorregirá.

6.2.3 Error en Tarjeta Madre o algún otro componente interno

Para reemplazar la tarjeta madre, tarjeta de memoria, fuente de poder, tarjeta de red,Controladora de discos o algún otro componente se deben tomar las siguientes acciones:

- *Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a directores y jefes de área.*
- *El servidor debe estar apagado, dando un correcto apagado del sistema.*
- *Preparar un nuevo equipo para reemplazar temporalmente el dañado donde se instalará y configurará todos los servicios de esa área.*
- *Hacer pruebas de funcionalidad.*
- *Notificar a los usuarios de que los servicios están en línea nuevamente.*

Nota: Todo cambio interno a realizarse en el servidor será fuera de horario laboral fijado por la dependencia, a menos que surja una dificultad que amerite cambiarlo inmediatamente.

6.2.4 Error Lógico de Datos

La ocurrencia de errores en los sectores del disco duro de los servidores puede deberse a una de las siguientes causas:

6.2.5 Caída del servidor por falla de la red.

Falla en el suministro de energía eléctrica por mal funcionamiento del Sistema de Alimentación Eléctrica Ininterrumpida (UPS).

Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna falla en los servidores de los sistemas computacionales de la Unidad de Gestión de la calidad e Informática, se debe tener en cuenta:

- *Verificar el suministro de energía eléctrica.*
- *Deshabilitar el ingreso de usuarios al sistema.*
- *Verificar que exista respaldo del servidor.*
- *Al término de la operación de reparación se procederá a revisar que las bases de datos índices estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente.*
- *Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilerías.*

En caso de producirse alguna vulneración o hackeo en los servidores de los Sistemas de Información de la Unidad de Gestión de la calidad e Informática, se debe tener en cuenta:

- *Aislar de la red de trabajo publica y local el equipo comprometido con la finalidad de contener la intromisión y evitar que esta se extienda a otros equipos de importancia.*
- *Identificar la vulneración por medio de las bitácoras de monitoreo de los equipos de seguridad, antivirus, log de equipos locales, para elaborar un plan de acción que permita atacar, restablecer y prevenir futuros ataques.*
- *Una vez identificada la grave del ataque, se deberá comunicar a los mandos directivos la situación y el plan de acción a tomar, indicando la severidad del ataque y el tiempo de restablecimiento de los servicios, así como*

indicar cuales servicio se mantendrán activos en un ámbito local de operación.

- *Comunicar a los usuarios de los accesos temporales que se habilitarán para permitir que la operatividad continúe.*
- *En caso de un ataque grave en el cual se requiera restablecer los servicios desde una instalación limpia, se revisaron los respaldos de servidor, aplicaciones y base de datos para asegurar que se tienen los más actuales y no están comprometidos, en caso de ser así se buscaran reestablecer con los respaldos que sigan en temporalidad.*
- *Restablecimiento de los servicios y aplicaciones de las medidas de prevención identificadas.*
- *Pruebas de funcionalidad en ámbito local y público de manera limitada.*
- *Comunicar a los usuarios del restablecimiento de los servicios.*
- *Monitoreo especializado en la situación durante un periodo de tiempo considerado para asegurar que la vulnerabilidad y las acciones preventivas funcionan de manera adecuada.*
- *Recursos de Contingencia*
- *Componente de remplazo (Memoria, Disco Duro, etc.).*

Plan de respaldos de la información del servidor (Procedimientos P-UGCI-SI-MBD-01 Respaldo de Información y Base de Datos y P-UGCI-SI-MBD-02 restauración de la Información en Base de Datos).

Interrupción del flujo eléctrico durante la ejecución de los procesos.

Actualmente no se cuenta con un respaldo de energía eléctrica por lo que se es necesario gestionar recursos para la adquisición de una planta de energía y equipos de Sistema de Alimentación Eléctrica Ininterrumpida (UPS).

RECURSOS DE CONTINGENCIA

Hay que asegurar que el estado de las baterías del Sistema de Alimentación Eléctrica Ininterrumpida (UPS) se encuentre en buen estado y siempre con cargada al tope.

Pérdida de servicio internet

Realizar pruebas para identificar posible problema dentro de la institución.

- Si se evidencia problema en el hardware, se procederá a *cambiar el componente.*
- *Si se evidencia problema con el software, se debe reinstalar el sistema operativo.*
- *Si no se evidencia falla en los equipos de la dependencia, se procederá a comunicarse con la empresa prestadora del servicio para asistencia técnica.*
- *Es necesario registrar en bitácora la avería para llevar un historial que servirá de guía para futuros daños.*
- *Realizar pruebas de operatividad del servicio.*
- *Aire de Precisión Site*
- *Mantenimientos periódicos semestral.*
- *Póliza anual de servicio y mantenimiento.*
- *Destrucción del Centro de Cómputo*
- *Contar con el inventario actualizado de sistemas informáticos.*
- *Identificar recursos de hardware y software que se puedan rescatar.*
- *Salvaguardar los respaldos de información previamente realizados.*
- *Identificar un nuevo espacio para restaurar el Centro de Cómputo.*
- *Presupuestar la adquisición de software, hardware, materiales, personal y transporte.*
- *Adquisición de recursos de software, hardware, materiales y contratación de personal.*
- *Iniciar con la instalación y configuración del nuevo centro de cómputo.*
- *Restablecer los respaldos realizados a los sistemas.*

7. PLAN DE RECUPERACION Y RESPALDO DE LA INFORMACION

El costo de la recuperación en caso de desastres severos, como los de un terremoto que destruya completamente el interior de edificios e instalaciones, estará directamente relacionado con el valor de los equipos de cómputo e información que no fueron informados oportunamente y actualizados en la relación de equipos

informáticos asegurados que obra en poder de la compañía de seguros. **Este plan de restablecimiento estratégico del sistema de red, software y equipos informáticos será abordado en la parte de Actividades Posteriores al Desastre.**

El paso inicial en el desarrollo del plan contra desastres es la identificación de las personas que serán las responsables de la ejecución del plan de contingencias. Por tanto, se definen los siguientes responsables:

- Coordinador de Infraestructura y Comunicación: Sera responsable de llevar a cabo las acciones correctivas definidas con anterioridad en lo que respecta a hardware y conectividad a fin de minimizar los riesgos establecidos.
- Coordinador de Sistemas de información: Sera responsable de llevar a cabo las acciones correctivas definidas con anterioridad en lo que respecta a software y bases de datos a fin de minimizar los riesgos establecidos.
- Titular de la Unidad de Gestión de la Calidad e Informática: Verificará la labor realizada por las Coordinaciones.

7.1 Procedimientos documentados en SICADIF

- *P-UGCI-SI-SOP-02 Revisión de Servidores*
- *P-UGIC-SI-MBD-01 Respaldos de Información de Base de Datos*
- *P-UGCI-SI-MBD-02 Restauración de la Información de Base de Datos.*

7.2 Clasificación del plan de recuperación y respaldo de la información.

Un Plan de Recuperación de Desastres se clasifica en tres etapas:

- *Actividades Previas al Desastre.*
- *Actividades Durante el Desastre.*
- *Actividades Después del Desastre.*

7.2.1 Actividades previas al desastre

Se consideran las actividades de resguardo de la información, en busca de un proceso de Recuperación con el menor costo posible para la Institución.

Se establecen los procedimientos relativos a:

- *Sistemas e Información.*
- *Equipos de Cómputo.*
- *Obtención y almacenamiento de los Respaldos de Información.*

a) Sistemas de Información

La institución deberá tener una relación de los Sistemas de Información y las bases de datos con los que cuenta, tanto los de desarrollo propio, como los desarrollados por empresas externas.

b) Equipos de Cómputo

Se debe tener en cuenta el inventario de hardware, impresoras, scanner, módems y otros, detallando su ubicación (software que usa, ubicación y nivel de uso institucional). Se deben emplear los siguientes criterios sobre identificación y protección de equipos:

- *Pólizas de seguros comerciales como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia, teniendo en cuenta la depreciación tecnológica.*
- *Señalización o etiquetamiento de las computadoras de acuerdo con la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación.*
- *Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la institución.*

c) Obtención y almacenamiento de copias de seguridad (Respaldos)

Se debe contar con procedimientos para la obtención de las copias de seguridad de todos los

elementos de software necesarios para asegurar la correcta ejecución de los sistemas en la institución.

Las copias de seguridad son las siguientes:

Respaldo del Sistema Operativo de servidores: Todas las versiones de sistema operativo de servidores instalados en la red. (Periodicidad - Diario).

Respaldo de los datos (Base de datos, password y todo archivo necesario para la correcta ejecución del software aplicativos de la institución). (Periodicidad -Diario y semanales).

7.2.2 Actividades Durante el Desastre (PLAN DE EMERGENCIAS)

Presentada la contingencia o desastre se debe ejecutar las siguientes actividades planificadas previamente:

Plan de Emergencias

La presente etapa incluye las actividades a realizar durante el desastre o siniestros, se debe tener en cuenta la probabilidad de su ocurrencia durante: el día, noche o madrugada. Este plan debe incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, descritas a continuación:

Buscar Ayuda de la Subsecretaria de Tecnologías de la Información y Comunicaciones (STICS) de la Secretaria de Hacienda del Gobierno del Estado.

Es de tener en cuenta que sólo se debe realizar acciones de resguardo de equipos en los casos en que no se pone en riesgo la vida de personas. Normalmente durante la acción del siniestro es difícil que las personas puedan afrontar esta situación, debido a que no están preparadas o no cuentan con los elementos de seguridad, por lo que las actividades para esta etapa del proyecto de prevención de desastres deben estar dedicados a buscar ayuda inmediatamente para evitar que la acción del siniestro cause más daños o destrucciones.

- *Se debe tener en toda oficina los números de teléfono y direcciones de organismos e instituciones de ayuda.*
- *Todo el personal debe conocer la localización de vías de escape o salida: Deben estar señalizadas las vías de escape o salida.*
- *Instruir al personal de la institución respecto a evacuación ante sismos, a través de*
- *simulacros, esto se realiza acorde a los programas de seguridad organizadas por Protección Civil a nivel local.*
- *Ubicar y señalizar los elementos contra el siniestro: tales como extintores, zonas de seguridad (ubicadas normalmente en las columnas), donde el símbolo se muestra en color blanco con fondo verde.*

- *Secuencia de llamadas en caso de siniestro: tener a la mano elementos de iluminación, lista de teléfonos de instituciones como: Compañía de Bomberos, Hospitales, Centros de Salud, Ambulancias, Seguridad.*

b) Formación de Equipos

Se debe establecer los equipos de trabajo, con funciones claramente definidas que deberán realizar en caso de desastre. En caso de que el siniestro lo permita (al estar en un inicio o estar en un área cercana, etc.), se deben formar dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y el otro para salvamento de los equipos informáticos, teniendo en cuenta la clasificación de prioridades.

c) Entrenamiento

Se debe establecer un programa de prácticas periódicas con la participación de todo el personal en la lucha contra los diferentes tipos de siniestro, de acuerdo con los roles que se hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se pueden realizar recarga de extintores, charlas de los proveedores, etc. Es importante lograr que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos; para estos efectos es conveniente que participen los directivos y ejecutivos, dando el ejemplo de la importancia que la alta dirección otorga a la seguridad institucional.

7.2.3 Actividades después del desastre

Estas actividades se deben realizar inmediatamente después de ocurrido el siniestro, son las siguientes:

a) Evaluación de daños

El objetivo es evaluar la magnitud del daño producido, es decir, qué sistemas se están afectando, qué equipos han quedado inoperativos, cuales se pueden recuperar y en cuanto tiempo. En el caso de la Unidad de Gestión de la Calidad e Informática se debe atender los procesos primordiales para el funcionamiento de

la institución, por la importancia estratégica. La recuperación y puesta en marcha de los servidores es prioritario.

b) Priorizar Actividades

La evaluación de los daños reales nos dará una lista de las actividades que debemos realizar,preponderando las actividades estratégicas y urgentes de nuestra institución. Las actividades comprenden la recuperación y puesta en marcha de los equipos de cómputo ponderado y los sistemas de información, compra de accesorios dañados, etc.

c) Ejecución de actividades

La ejecución de actividades implica la colaboración de todos los usuarios, creando equipos de trabajo asignando actividades. Cada uno de estos equipos deberá contar con un líder que deberá reportar el avance de los trabajos de recuperación y en caso de producirse un problema, reportarlo de inmediato al directivo brindando posibles soluciones.

Los trabajos de recuperación se iniciarán con la restauración del servicio usando los recursos de la dependencia, teniendo en cuenta que en la evaluación de daños se contempló y gestionó la adquisición de accesorios dañados.

La segunda etapa es volver a contar con los recursos en las cantidades y lugares

propios del sistema de información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad de la dependencia y el buen servicio de nuestro sistema e imagen institucional.

d) Evaluación de Resultados

Una vez concluidas las labores de recuperación de los sistemas que fueron afectados por el siniestro, debemos de evaluar objetivamente todas las actividades realizadas, con qué eficacia se hicieron, cuánto tiempo tomaron, qué circunstancias modificaron (aceleraron o entorpecieron) las actividades, cómo se comportaron los equipos de trabajo, etc. De la evaluación de resultados y del siniestro, deberían obtenerse dos tipos de recomendaciones; una, la retroalimentación del Plan de Contingencias y Seguridad de Información; y otra, una lista de

recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

e) Retroalimentación de Actividades

Con la evaluación de resultados podemos mejorar las actividades que tuvieron algún tipo de dificultad y reforzarlos elementos que funcionaron adecuadamente.

8. CONCLUSIONES

El presente Plan de contingencias y Seguridad en Información de la Dirección General de Informática, tiene como fundamental objetivo el salvaguardar la infraestructura de la Red y Sistemas de Información.

Este Plan está sujeto a la infraestructura física y las funciones que realiza la Unidad de Gestión de la Calidad e Informática. El Plan de Contingencias, es un conjunto de procedimientos alternativos al orden normal de una institución, cuyo fin es permitir su funcionamiento continuo, aun cuando alguna de sus funciones se viese dañada por un accidente interno o externo. Que una institución prepare su Plan de Contingencia, supone un avance a la hora de contrarrestar cualquier eventualidad, que puedan acarrear importantes pérdidas y llegado el caso no solo material sino personales y de información.

Las principales actividades requeridas para la implementación del Plan de Contingencias son: Identificación de riesgos, Minimización de riesgos, Identificación de posibles eventos para el Plan de Contingencia, Establecimiento del Plan de Recuperación y Respaldo, Plan de Emergencias y Verificación e implementación del plan.

9. RECOMENDACIONES

Hacer de conocimiento general el contenido del presente Plan de Contingencias y Seguridad de Información, con la finalidad de instruir adecuadamente al personal de la Unidad de Gestión de la Calidad e Informática.

Adicionalmente al plan de contingencias se deben desarrollar las acciones correctivas planteadas para minimizar los riesgos identificados.

Es importante tener actualizados los contratos de garantía y licencias tanto de hardware como de software, así como pólizas de aseguramiento.

Es importante puntualizar la necesidad de contar con una planta de energía de respaldo y con los Sistema de Alimentación Eléctrica Ininterrumpida (UPS) para evitar la suspensión de los servicios y asegurar la continuidad de las operaciones, especialmente en situaciones donde el suministro eléctrico principal falla o es interrumpido.

Actualmente los servidores de aplicaciones y base de datos se encuentra en localizados en dos ubicaciones distintas, una administrada directamente por el personal de la Coordinación de Tecnologías de la Información y Comunicaciones en el Site ubicado en las oficinas de la Unidad de Gestión de la Calidad e Informática (UGCI); la segunda ubicación es el Site de datos de la Subsecretaria de Tecnologías de la Información y Comunicaciones la Secretaria de Hacienda del Gobierno del Estado,el cual es administrado por personal de dicha dependencia, lo cual limita la actuación y administración sobre los equipos de servidores que se encuentran ahí; es importante señalar que recientemente se nos ha solicitado preparar un proyecto de migración para que los servidores que se mantienen ahí sean reubicados al Site de datos de la y UGCI, lo cual impacta en reforzar los siguientes puntos:

- *Suministro de energía de respaldo y unidas de energía ininterrumpida.*
- *Reforzar la seguridad de la red interna y perimetral, con equipos tipo firewall actualizados.*
- *Climatización adecuada del site de datos.*
- *Cableado estructurado y certificado.*
- *Contratar servicios de telecomunicaciones e internet con mayor alcance.*