PLAN DE CONTINGENCIAS DE EQUIPOS Y SISTEMAS INFORMÁTICOS

DIRECCIÓN GENERAL DE INFORMÁTICA

INTRODUCCIÓN

El Plan de Contingencias de Equipos y Sistemas Informáticos de la Dirección General de Informática, 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.

OBJETIVO

El principal objetivo de un Plan de Contingencias de la Dirección General de Informática es la de garantizar la continuidad de las operaciones dentro de la institución.

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 Dirección General de Informática.

IDENTIFICACIÓN DE PROCESOS Y SERVICIOS

Principales Procesos de Software Identificados Software

- YOREMIA (control escolar)
- PrepaSon
- FUP (personal)
- Cédulas profesionales
- Nómina
- Contabilidad
- Asignación de plazas
- POSSSES
- Ingresos propios
- SIIICASF
- SAPEIB
- SAIS
- Gestión Documental
- Uniformes escolares

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.

ANÁLISIS DE EVALUACIÓN DE RIESGOS Y ESTRATEGIAS

Metodología aplicada

Para la clasificación de los activos de las Tecnologías de Información de la Dirección General de Informática se han considerado tres criterios:

Grado de negatividad: Un evento se define con grado de negatividad (Leve, moderada, grave y muy severo).

Frecuencia del Evento: Puede ser (Nunca, aleatoria, periódico y continuo)

Impacto: El impacto de un evento puede ser (Leve, moderado, grave y muy severo).

Plan de Contingencias

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.)

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: como actos terroristas, desórdenes, 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).

Clases de Riesgos

- Incendio o Fuego
- Robo común de equipos y archivos
- Falla en los equipos
- Equivocaciones
- Acción virus informático
- Fenómenos naturales
- Accesos no autorizados
- Ausencia del personal de sistemas.

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, nuestra región, ha registrado en estos últimos tiempos lluvias fuertes, las que podrían producir mayores estragos, originando filtraciones de agua en los edificios y techos, así como inundaciones, produciendo cortes de luz, cortos circuitos (que podrían desencadenar en incendios).

Incendio o Fuego
Grado de Negatividad: Muy Severo
Frecuencia de Evento: Aleatorio
Grado de Impacto: Alto

Situación Actual	Acción Correctiva
La oficina donde están ubicados los servidores cuenta con un extintor cargado, ubicado de manera estratégica. De igual forma cada oficina cuenta con un extintor debidamente cargado.	Se cuenta con un sistema de detección, control y sofocación contra incendios.
Se ha ejecutado un programa de capacitación sobre el uso de elementos de seguridad y primeros auxilios, a los funcionarios.	Se cumple
El servidor realiza respaldos de la información diariamente, pero no existe ninguna otra copia de respaldo.	Realizar respaldos del servidor en ubicaciones remotas con la finalidad de tener un respaldo dual en por lo menos dos (2) sitios distintos. Además se cuenta con un DRP en las instalaciones del C5 de la SSP.

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, tal 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.

Robo Común de Equipos y Archivos
Grado de Negatividad: Grave
Frecuencia de Evento: Aleatorio
Grado de Impacto: Moderado

Situación Actual	Acción Correctiva
Debido a que a la hora de salida de las personas particulares que ingresan a la institución, no son registradas pues no se cuenta con vigilante. Cabe anotar que contamos con sistema de seguridad para la entrada y salida del personal.	Se requiere que cada funcionario en el momento de retirarse de la oficina por un tiempo considerable opte por guardar su equipo dentro de algún cajón bajo llave.
Autorización escrita firmada por el jefe de área, técnico de soporte y funcionario	Se cumple por medio del formato establecido para salida de equipos.

responsable, para la salida de equipos de la institución.	

No se han reportado casos en la cual haya existido manipulación y reubicación de equipos sin el debido conocimiento y autorización del jefe de cada área y el técnico de soporte, esto demuestra que los equipos se encuentran protegidos por cada funcionario autorizado de la institución.

Según antecedentes de otras unidades administrativas, es de conocer que el robo de accesorios y equipos informáticos, llegaron a participar personal propio de la institución en colusión con el personal de vigilancia, es relativamente fácil remover un disco duro del CPU, una lectora, tarjeta, etc. y no darse cuenta del faltante hasta días después. Estas situaciones no se han presentado en nuestra dependencia, pero se recomienda siempre estar alerta.

Falla en los Equipos
Grado de Negatividad: Grave
Frecuencia de Evento: Aleatorio Grado de Impacto: Grave

Situación Actual	Acción Correctiva
La falla en los equipos muchas veces se debe a falta de mantenimiento y limpieza.	Se cumple. Se realiza mantenimiento preventivo de equipos por lo menos dos veces al año.
La falla en el hardware de los equipos requiere de remplazo de repuestos de forma inmediata.	Se cumple. Se cuenta con proveedores en caso de requerir remplazo de piezas y en ocasiones es posible contar con repuestos de quipos que están para darse de baja. Gestión de garantía vigente.
Cada área funcional se une a la Red a través gabinetes, la falta de energía en éstos origina la ausencia de uso de los servicios de red.	Se cumple. Los gabinetes se encuentran protegidos en un lugar de acceso restringido y son manipulados solo por personal técnico del área de informática.
El daño de equipos por fallas en la energía eléctrica requiere contar con dispositivos que amplíen tiempo para apagar correctamente el equipo.	Se cumple. La Dirección General de Informática cuenta con UPS, el cual provee de energía de respaldo para realizar el debido apagado del equipo en caso de presentarse falla eléctrica.

Teniendo en cuenta la importancia del fluido eléctrico para el funcionamiento del área, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolongara por tiempo indefinido provocaría un trastorno en las operaciones del día, sin afectar los datos. 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.

Termo magnéticos

Si una parte de una computadora funde un fusible o hace saltar un diferencial, primero se debe desconectar el equipo, a continuación, debe desconectarse el cable de alimentación eléctrica que lleva al equipo y buscar la falla que ha hecho saltar el termomagnético. Una vez arreglado el problema se puede volver a conectar el equipo. Al restablecer el circuito eléctrico, se ha de tener cuidado que todos los equipos deben estar apagados y desconectados antes de cambiar el mismo. No se debe olvidar que algunos elementos del equipo, como es el caso de los monitores, pueden mantener una carga de alto voltaje incluso, después de haberse apagado, asegurarse que el fusible de recambio es de la misma capacidad que el fundido. No aprobar las reparaciones de los termomagnéticos, usando hilos de cobre o similares.

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.

Equivocaciones manejo del sistema Grado de Negatividad: Moderado Frecuencia de Evento: Periódico Grado de Impacto: Moderado

Situación Actual	Acción Correctiva
Equivocaciones que se producen de forma involuntaria, con respecto al manejo de información, software y equipos.	Se cumple. Se realiza una instrucción inicial en el ambiente de trabajo presentando las políticas informáticas establecidas para manejo de sistemas.
En ocasiones el usuario que tiene conocimiento en informática intenta navegar por sistemas que no están dentro de su función diaria.	Se cumple. El encargado de sistemas asigna permisos y privilegios a cada usuario de acuerdo con sus funciones.
La entrega de inventario es realizada por el área de almacén no se realiza de forma mancomunada con el área de informática.	Se cumple. El área de almacén entrega inventario junto con el encargado de sistemas en lo referente a equipos de cómputo, licencias, antivirus y solicitar la creación inmediata del usuario con sus claves.
El daño de equipos por fallas en la energía eléctrica requiere contar con dispositivos que amplíen tiempo para apagar correctamente el equipo.	Se cumple. La Dirección General de Informática (DGI) cuenta con UPS, equipo que provee de energía de respaldo para realizar el debido apagado del equipo en caso de presentarse falla eléctrica.
Se presentan equivocaciones en el manejo de información debido a que no existen políticas de informática claras y precisas.	Se cumple. Existen políticas de informáticas claras y precisas, las cuales se les comunican a los usuarios al igual que cualquier modificación a las mismas.

Acción de Virus Informático Grado de Negatividad: Muy Severo Frecuencia de Evento: Continuo Grado de Impacto: Grave

Situación Actual	Acción Correctiva
Se cuenta con un software antivirus para la institución, pero su actualización no se realiza de forma inmediata a su expiración.	Se debe evitar que las licencias de antivirus expiren, se requiere renovación con anterioridad del antivirus.
Únicamente el área de informática es la encargada de realizar la instalación de software en cada uno de los equipos de acuerdo con su necesidad.	Se cumple. El ingeniero de soporte técnico tiene una cuenta con derechos administrativos sobre los equipos de cómputo.
Se tiene acceso restringido al servidor, únicamente es el administrador de la red el encargado de cambiar configuraciones y anexar nuevos equipos.	Antes de ingresar una maquina a la red, se debe comprobar la no existencia de virus en la misma.

Por medio del correo electrónico se obtienen virus constantemente.	Se cumple. Se cuenta con un correo institucional para cada usuario, de manera que únicamente se reciba información de importancia para la institución. Existen filtros de seguridad.
Los antivirus no se actualizan periódicamente en cada equipo.	Se cumple. Se mantiene constante revisión a través de la consola de antivirus.

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.

Fenómenos Naturales

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

Situación Actual	Acción Correctiva
En la última década no se han registrado urgencias por fenómenos naturales como terremotos o inundaciones.	Aunque la probabilidad de ocurrencia es baja se requiere tener en cuenta medidas de prevención.
Aunque existen épocas de lluvia fuertes, las instalaciones de la DGI están debidamente protegidas.	Tomar medidas de prevención
Los servidores principales se encuentran en un ambiente libre de filtraciones.	Ante la mínima filtración se debe informar de inmediato a la dirección, para realizar el respectivo mantenimiento preventivo.

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.

Accesos No Autorizados

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

Situación Actual	Acción Correctiva

Se controla el acceso al sistema de red mediante la definición de un administrador con su respectiva clave.	Se cumple. Mediante la generación de usuarios y contraseñas, mediante el servicio de directorio de Active Directory Domain Services.
La asignación de usuario se realiza a discrecionalidad del encargado de seguridad de la DGI y se solicita de forma escrita.	Se cumple. Se solicita por escrito (E-mail) al encargado de sistemas la creación de usuarios y los permisos que se requiere sean asignados, o cualquier cambio referente a los mismos.
La oficina administrativa no comunica al área de sistemas, cuando un funcionario sale a vacaciones o se retira de la institución a fin de desactivar ese usuario.	Se debe informar a la Dirección General de Informática que funcionario sale a vacaciones para así bloquear el respectivo usuario por el tiempo de ausencia, igualmente en caso de retiro definitivo.
Se acostumbra a confiar la clave de acceso (uso personal) a compañeros de área, sin medir la implicación en el caso de acceso no autorizado.	Capacitar al personal sobre la confidencialidad de sus contraseñas, resaltando la responsabilidad e importancia que ello implica, sobre todo, para el manejo de software.
No se cancelan los usuarios del personal que se retira de la institución de forma inmediata, recurriendo en algunos casos a utilizar la contraseña del funcionario ausente.	Tan pronto se informe que un funcionario se retira definitivamente se debe cancelar este usuario. Apegarse a política de baja de usuario.

Ausencia del personal de sistemas Grado de Negatividad: Grave Frecuencia de Evento: Aleatorio Grado de Impacto: Grave

Situación Actual	Acción Correctiva
En la DGI existe un único funcionario con autorización para administrar los sistemas.	Es importante autorizar un administrador del sistema alterno, en caso de que falte el funcionario de sistemas no se paralice la institución.
El funcionario de informática es la única persona con claves de acceso al sistema, conocedor del manejo de la red y los sistemas de información.	El funcionario de informática impartirá instrucciones al administrador alterno.
El administrador alterno necesitara conocer el inventario actualizado de sistemas.	Realizar depuración al inventario de sistemas, realizando devolución de los equipos en comodato que no están siendo utilizados.
Existe relación de los sistemas de información con los que cuenta la institución y su utilidad.	Se cumple. Se tiene un inventario de los sistemas de información de la institución, detallando usuarios, en que equipos están instalados y utilidad.
En caso de fallas en la red y ausencia del funcionario de sistemas, existe un diagrama lógico en el cual se definen las conexiones de red existentes, de forma que se agiliza la labor de recuperación del sistema.	Se cumple. Se cuenta con diagrama lógico de la red y diagrama físico de cada uno de los puntos de red para que en caso de falla se agilice el trabajo de inspección y por ende la recuperación del sistema.

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.

RIESGO	EVENTO
• Fallas Corte de Cable UTP. • Fallas Tarjeta de Red. • Fallas IP asignado. • Fallas Punto de Switch. • Fallas Punto Patch Panel. • Fallas Punto de Red. • Falla en la conectividad de Fibra Óptica	No existe comunicación entre cliente y servidor. Al perder conexión la FO deja de haber comunicación entre edificios.
• Fallas de Componentes de Hardware del Servidor. • Falla del UPS (Falta de Suministro eléctrico). • Virus. • Sobrepasar el límite de almacenamiento del Disco • Computador de escritorio funciona como servidor.	Fallas en el equipo servidor.
• Incapacidad. • Accidente. • Renuncia Intempestiva.	Ausencia parcial o permanente del personal de tecnología de la información.
• Corte General del Fluido eléctrico	Interrupción del fluido eléctrico durante la ejecución de los procesos.
• Falla de equipos de comunicación: Switch, Antenas. • Falla Fibra Óptica. • Fallas en el Software de Acceso a Internet. • Pérdida de comunicación con proveedores de Internet.	Pérdida de servicio de internet.
• Incendio • Sabotaje • Corto Circuito • Terremoto	Indisponibilidad de la sala de servidores.

No hay comunicación entre Cliente – Servidor en la Dirección General de Informática

Existe el servicio de Mesa de Ayuda de Informática, la cual se activa al realizar una llamada telefónica por parte del usuario afectado, al número de extensión es la 6000. Ahí se levantará un reporte en el Sistema Service Desk con el que se atenderá el requerimiento del usuario.

- Requerimiento del usuario que no cuenta con acceso a la red.
- El ingeniero de soporte a quien se le asignó el reporte procederá a identificar el problema.
- Si se detecta problema con el Patch Cord, realizar cambio de éste.
- Si no se resuelve el problema revisar si existe problema en la tarjeta de red, en caso de afirmativo realizar cambio o arreglo de ésta.

- Si persiste el problema revisar los puntos de red, utilizando el diagrama lógico.
- Testear el cable UTP. Si existe daño, realizar el cambio del cable.
- Realizar mantenimiento del punto de red del usuario y del gabinete de comunicaciones.
- Recuperación del sistema de red para el usuario.

Recursos de Contingencia

- Componentes de remplazo.
- Diagrama lógico de la red.

Falla del 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:

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.

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 correctchecking), por tanto, si hubiese un error de paridad, el servidor se autocorregirá.

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.
- Ubicar la posición de la pieza a cambiar.
- Retirar la pieza con sospecha de deterioro y tener a la mano otra igual o similar.
- Retirar la conexión de red del servidor, ello evitará que, al encender el sistema, los usuarios ingresen.
- Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.

- Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

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.

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:

- Caída del servidor de archivos por falla de software de red.
- Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.
- Bajar incorrectamente el servidor de archivos.
- 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 DGI, se debe tener en cuenta:

- Verificar el suministro de energía eléctrica.
- Deshabilitar el ingreso de usuarios al sistema.
- Realizar respaldo de archivos contenidos en el servidor, a excepción de la carpeta raíz.
- 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.

Recursos de Contingencia

- Componente de remplazo (Memoria, Disco Duro, etc.).
- Plan de respaldos de la información del servidor.

Ausencia parcial o permanente del personal.

- Instrucción del Director del Área (escrita o Email) para que el **administrador** alterno se encargue del centro de cómputo de la DGI especificando el periodo de asignación.
- Obtener la relación de los sistemas de información con los que cuenta la DGI, detallando usuarios, en que equipos se encuentran instalados y su utilidad.
- Conocer la ubicación de los respaldos de información.
- Contar con el diagrama lógico de red actualizado.

Recursos de Contingencia

- Manual de funciones actualizado del encargado de sistemas de la DGI.
- Relación de los sistemas de información de la DGI.
- Diagrama lógico actualizado de la red de la dependencia.

Interrupción del fluido eléctrico durante la ejecución de los procesos.

- Si fuera corto circuito, el UPS mantendrá activo los servidores mientras se repare la avería eléctrica.
- A los 8 segundos del corte de energía eléctrica de la red pública, encenderá la Planta de Energía de respaldo, misma que alimentará el UPS durante el tiempo que dure ese corte de energía pública. Es bien importante estar pendiente del nivel de combustible (Diesel) ya que de eso depende que la Planta se mantenga encendida.
- Para el caso de apagón se mantendrá la autonomía de corriente que el UPS nos brinda (corriente de emergencia), hasta que los usuarios completen sus operaciones, para que no corten bruscamente el proceso que tienen en el momento del apagón.

- Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso del UPS a corriente normal (Corriente brindad por la empresa eléctrica).
- Con el regreso del servicio de energía eléctrica de la red pública, se invierte el suministro de corriente hacia el UPS y la Planta Eléctrica de respaldo se apagará a los 8 minutos para pasar al estado de Stand By (Espera) nuevamente.

Recursos de contingencia

- Hay que asegurar que el estado de las baterías del 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.
- Servicio de internet activo.

Aire de Precisión Site

- Mantenimientos periódicos semestral.
- Póliza anual de servicio y mantenimiento.
- Monitorear vía web los valores y estándares según las Normas Oficiales para Centros de Datos y Arreglos de Servidores.

Recursos de Contingencia

- Hardware.
- Router.
- Software.
- Herramientas de Internet.

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.

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:

Encargado de Sistemas: Sera responsable de llevar a cabo las acciones correctivas definidas con anterioridad a fin de minimizar los riesgos establecidos.

Director de Área: Verificará la labor realizada por el Encargado de Sistemas.

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

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

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 dependencia. 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 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. Por ejemplo, etiquetar de color rojo los servidores, color amarillo a los PC con información importante o estratégica, y color verde a las demás estaciones (normales, sin disco duro o sin uso).
- 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: Todas las versiones de sistema operativo instalados en la red. (Periodicidad – Semestral).
- Respaldo de los datos (Base de datos, password y todo archivo necesario para la correcta ejecución del software aplicativos de la institución). (Periodicidad – Mensual).

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:

a. Buscar Ayuda de Otros Entes

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 Defensa Civil a nivel local u otros entes.
- 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.

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 DGI 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 reforzar los elementos que funcionaron adecuadamente.

FUNCIONES

PUESTO	FUNCIÓN
Director de Sistemas Operativos y Comunicaciones.	Administrar el resguardo de la información integrada en la infraestructura de SEC/SEES.
Director de Sistemas Operativos y Comunicaciones.	Actualizar el documento Plan de Contingencia.
Director de Sistemas Operativos y Comunicaciones.	Resguardar el documento Plan de Contingencia.

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 el Área de Sistemas.

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.

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 Dirección General de 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.

Cuando el administrador de la red se encuentre ausente se recomienda capacitar a una persona que pueda hacer lo mínimo indispensable para levantar todos los servicios, a fin de que la operación básica de la institución no se vea interrumpida.