Instituto de Pensiones del Estado de Veracruz

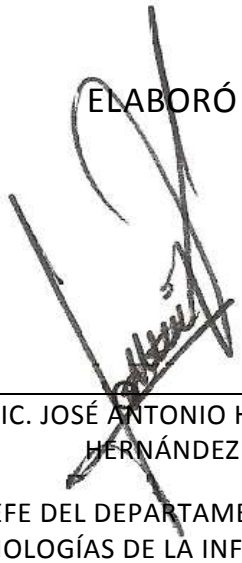
VERACRUZ
GOBIERNO DEL ESTADO

PLAN DE CONTINGENCIAS

Septiembre 2014

FIRMAS DE AUTORIZACIÓN

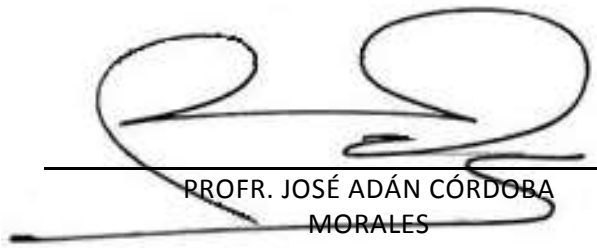
ELABORÓ



LIC. JOSÉ ANTONIO HUERTA HERNÁNDEZ

JEFE DEL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN

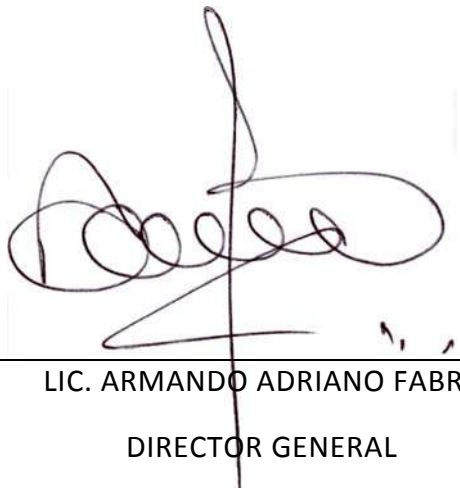
REVISÓ



PROFR. JOSÉ ADÁN CÓRDOBA MORALES

SUBDIRECTOR ADMINISTRATIVO

AUTORIZÓ



LIC. ARMANDO ADRIANO FABRE

DIRECTOR GENERAL

ÍNDICE

INTRODUCCIÓN 3

OBJETIVO 4

ALCANCE 4

ORGANO RESPONSABLE 4

MARCO DE REFERENCIA 4

DEFINICIONES DE TÉRMINOS EMPLEADOS 5

ESCENARIOS DE CONTINGENCIA 6

ETAPAS DEL PLAN 6

RECURSOS 7

ANÁLISIS DE RIESGOS 7

- FALLA DE EQUIPO DE COMUNICACIÓN (Tipo de Impacto Alto) 8
- FALLA DE SERVIDOR DE RED (Tipo de Impacto Alto) 8
- ACCESO A LA RED NO AUTORIZADO (Tipo de Impacto Alto) 9
- ATAQUE DE VIRUS INFORMÁTICO (Tipo de Impacto Medio) 9
- FALLAS DE ENERGÍA ELÉCTRICA (Tipo de Impacto Alto) 10
- EVENTO POLÍTICO-SINDICAL y SINIESTRO NATURAL (Tipo de Impacto Alto) 11

PLAN DE RESPALDOS 11

PLAN DE MANTENIMIENTO 12

PLAN DE ENTRENAMIENTO 13

CONSIDERACIONES Y ACTIVIDADES PREVENTIVAS 13

PLAN DE CONTINUIDAD 16

INTRODUCCIÓN

El Instituto de Pensiones del Estado en su afán por ir mejorando día a día los servicios que presta a sus derechohabientes, ha venido haciendo esfuerzos por mantenerse a la vanguardia en materia de las tecnologías de la información, sobre la cual, apoya en gran parte su aparato administrativo. Dentro de este Instituto existe el Departamento de Tecnologías de la Información (DTI), el cual es responsable de mantener en óptimo funcionamiento esta Infraestructura Tecnológica Informática, y salvaguardar la integridad de la información electrónica Institucional alojada en los servidores de aplicaciones.

Como parte del cumplimiento de esta responsabilidad, el Departamento de Tecnologías de la Información, ha elaborado el presente “Plan de Contingencias y Recuperación de Desastres”, con el fin de coadyuvar en el pronto restablecimiento de los servicios informáticos, ante la presencia de una contingencia.

En el presente Plan se han definido nuevas estrategias de operación, en relación con el natural comportamiento evolutivo de las tecnologías de la información, dentro del ciclo de vida iterativo “plan-do-check-act”, es decir, "planifica-actúa-comprueba-corrige".

OBJETIVO

Contar con un instrumento documental que actúe como referencia y guía de las actividades a realizarse, en caso de presentarse una contingencia en las instalaciones del Instituto de Pensiones del Estado, el cual permita restaurar los servicios de la red de cómputo de forma rápida y eficiente.

ALCANCE

Este Plan contempla el actuar del personal del Departamento de Tecnologías de la Información, ante la presencia de una contingencia, en las oficinas centrales del Instituto de Pensiones del Estado de Veracruz, conformado por los edificios A, B, C, y D. Ubicado en la calle Arco Vial Sur No. 730, Colonia Lomas Verdes en la ciudad de Xalapa.

En el presente se están considerando afectaciones que pudieran darse, de manera directa e indirecta, a la infraestructura tecnológica instalada en estas instalaciones.

ORGANO RESPONSABLE

Departamento de Tecnologías de la Información, adscrito a la Subdirección Administrativa.

MARCO DE REFERENCIA

El Instituto de Pensiones del Estado cuenta con una red de datos instalada en los edificios A, B, C, y D de sus oficinas centrales. Cada uno de los edificios, cuenta con cableado estructurado categoría 6 constituido con cable de cobre UTP y fibra óptica, red de energía eléctrica regulada exclusiva para equipos de cómputo, un IDF (Intermediate Distribution Frame) por cada nivel, oficinas

con equipos de cómputo: Computadoras, Impresoras, Multifuncionales, Escaners, Equipos de comunicación, etc.

En la planta baja del edificio C, dentro del Departamento de Tecnologías de la Información, está ubicado el cuarto principal de comunicaciones denominado comúnmente "SITE de Servidores". En él se encuentra instalado un rack con cuatro servidores tipo Blade y dos más de escritorio, además del MDF (Main Distribution Frame).

DEFINICIONES DE TÉRMINOS EMPLEADOS

Contingencia: Interrupción no planificada de la disponibilidad de recursos informáticos.

Plan de Contingencia: Son procedimientos que definen cómo una institución o negocio, continuará o recuperará sus funciones críticas en caso de una interrupción no planeada.

Proceso crítico: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la entidad, y cuya falta o ejecución deficiente puede tener un impacto operacional o de imagen significativo para la institución.

Impacto: El impacto de una actividad crítica se encuentra clasificado, dependiendo de la importancia dentro de los procesos TI, en:

Impacto Alto: Se considera que una *actividad* crítica tiene impacto alto sobre las operaciones de la entidad cuando ante una eventualidad en ésta *se encuentran imposibilitadas para realizar sus funciones normalmente*.

Impacto Medio: Se considera que una *actividad* crítica tiene un impacto medio cuando la falla de ésta, *ocasiona una interrupción en las operaciones de la entidad por un tiempo mínimo de tolerancia*.

Impacto Bajo: Se considera que una *actividad* crítica tiene un impacto bajo, cuando la falla de ésta, *no tiene un impacto en la continuidad de las operaciones de la entidad*.

ESCENARIOS DE CONTINGENCIA

Son considerados escenarios de contingencia para este Plan, entre otros, los siguientes casos:

1.- La no disponibilidad de algún servicio informático proporcionado mediante la red de datos: Sistemas de Información, de Impresión, Internet, Correo Electrónico, Intercambio Electrónico de Archivos, Enlaces Digitales e Intercomunicación Electrónica.

2.- El no acceso a las oficinas centrales del Instituto por diversas causas: Políticas, Organizacionales, Siniestro, etc.

3.- La pérdida parcial o total, del edificio donde se encuentra ubicado el SITE de Servidores o de algún otro edificio que conforman las oficinas centrales del Instituto.

4.- Pérdida de algún equipo de cómputo con funciones de misión críticas (de comunicación, procesamiento, etc.).

5.- Sabotaje físico o electrónico informático.

ETAPAS DEL PLAN

-Análisis de Riesgos
-Plan de Respaldos
-Plan de Recuperación
-Plan de Mantenimiento
-Plan de Entrenamiento

RECURSOS

HUMANOS

-Personal del Departamento de Tecnologías de la Información.

TÉCNICOS

- Switch de 48 Ptos., Velocidad 10/100 o mayor de preferencia.
-Equipo de respaldo de energía eléctrica (nobreak) con capacidad de 750 wats o mayor.
-Servidor de Aplicaciones con capacidad para soportar sistema operativo de red Windows 2008 Srv. y manejador de base de datos.
-Computadora de escritorio con sistema operativo Windows Seven.
-Respaldos de información electrónica manejada por los sistemas de información, de fecha lo más reciente posible.

ANÁLISIS DE RIESGOS

El impacto de una actividad crítica se encuentra clasificado, dependiendo de la importancia dentro de los procesos en TI, con la siguiente escala:

TABLA DE RIESGOS	
Tipo	**Factor**
Falla de Equipo de Comunicación	Alto
Falla de Servidor de Red	Alto
Acceso a la Red No Autorizado	Alto
Ataque de Virus Informático	Medio
Fallas de Energía Eléctrica	Alto
Imposibilidad de acceso a las instalaciones	Alto
Siniestro Natural	Alto

FALLA DE EQUIPO DE COMUNICACIÓN (Tipo de Impacto Alto)

1.- Identificar el Tipo de equipo de comunicación que presenta daño.

2.- Reemplazarlo por otro de similares características.

3.- Integrarlo a la señal de Red mediante cable UTP o de Fibra Óptica según lo permita su tipo de conectividad.

4.- Hacer las pruebas de funcionalidad y verificar que todas las estaciones de trabajo conectadas a este equipo tengan señal de red.

5.- Realizar los trámites administrativos correspondientes para reparar el quipo dañado.

6.- Reintegrar el equipo reparado no sin antes haya sido probada su completa funcionalidad, en horarios que no afecte las actividades de los usuarios.

FALLA DE SERVIDOR DE RED (Tipo de Impacto Alto)

1.- Revisar las alertas del sistema de servidores.

2.- Identificar el servidor que esté presentando los problemas.

3.- Debido al esquema redundante de servidores con que se cuenta actualmente, verificar que los servicios sigan funcionando.

4.- Proceder a la intervención del servidor con problemas, considerando no interferir con los servicios en operación.

5.- Reintegrar el servidor intervenido al sistema en horarios fuera de servicios laboral.

ACCESO A LA RED NO AUTORIZADO (Tipo de Impacto Alto)

El acceso a la red de datos está controlado mediante el otorgamiento de cuenta y password personalizado, seguridad antivirus y de seguridad perimetral para el acceso desde internet, sin embargo, como todo sistema electrónico no se está exento de la proliferación de algún posible intruso. Por lo que en estos casos se debe proceder a lo siguiente:

1.-. Detener todo servicio que se note con comportamiento anormal.

2.- De ser necesario bloquear todo acceso al sistema de base de datos, sistemas de información y de servidores.

3.- Monitorear la actividad que se está registrando.

4.- Eliminar toda cuenta que se considere sospechosa hasta lograr la estabilidad en los servicios.

5.- Desconectar físicamente de la red de datos, toda computadora o servidor que presente comportamiento extraño, y realizarle las pruebas de funcionalidad adecuadas.

6.- Reintegrar los servicios o equipos desconectados a la red, una vez que se esté seguro de buen funcionamiento.

7.- En caso de identificar plenamente al intruso, hacer del conocimiento a las autoridades administrativas de este Instituto, para los efectos procedentes.

ATAQUE DE VIRUS INFORMÁTICO (Tipo de Impacto Medio)

El Instituto cuenta con el software de seguridad antivirus, para los servidores y las estaciones de trabajo; asimismo a través de la red, se

hacen las actualizaciones del antivirus hacia todas las máquinas que conforman la red de datos.

Sin embargo, en caso de infección de virus se deben de tomar las siguientes acciones:

1.- Revisar las alertas que envía el antivirus y ver el tipo de virus que se está propagando detectando el origen del virus. A su vez desconectar de la red el o los equipo que están infectando y que está reenviando el virus.

2.- Proceder a limpiar los archivos de las máquinas infectadas mediante el software antivirus, asegurándose de activar la opción de “Limpiar o Eliminar los archivos infectados”.

3.- Si no se logran limpiar los archivos infectados, proceder a reinicializar la máquina con fuentes de software seguros.

4.- Reintegrar las máquinas intervenidas a la red y monitorear su correcto funcionamiento.

FALLAS DE ENERGÍA ELÉCTRICA (Tipo de Impacto Alto)

Todo equipo de cómputo cuenta con su propio dispositivo de respaldo de energía eléctrica (UPS).

1.- Revisar la carga del UPS que alimentan los servidores de red, para los casos de corte de energía y determinar el tiempo que queda de energía auxiliar.

2.- Llamar al Departamento de Servicios Generales para conocer el origen de la falla y tiempo estimado de suspensión.

3.- Dependiendo del comportamiento del servicio de energía eléctrica, tomar la decisión de apagar todo el sistema de servidores de red y desconectarlo del toma corriente.

4.- Realizar los avisos pertinentes a los usuarios de todas las áreas del Instituto, para hacerles de su conocimiento del fenómeno presentado.

5.- Esperar el aviso por parte del Departamento. de Servicio Generales para reanudar el servicio de red.

6.- Reanudar el servicio de la red de datos, toda vez que se haya estabilizado el servicio de energía eléctrica, y notificarle al usuario para que continúe con sus actividades.

IMPOSIBILIDAD DE ACCESO A LAS INSTALACIONES (Tipo de Impacto Alto)

La ocurrencia de ambos eventos tendría como consecuencia el No acceso, total o parcial, a las oficinas del Instituto y por ende a su red de datos, por lo cual se tienen contempladas acciones para enfrentar este tipo de acontecimientos, mismas que están descritas más adelante en el rubro de “Plan de Continuidad” de este mismo documento.

PLAN DE RESPALDOS

El modelo de respaldos implementado para la salvaguarda de la información electrónica contenida en los servidores de la red de datos, consiste en realizarlo en cuatro diferentes medios de almacenamiento removibles, por el Departamento de Tecnologías de la Información, como se define a continuación:

TIPO DE RESPALDO	UBICACIÓN
Permanente	Caja de Seguridad Bancaria
Actualizable	Caja de Seguridad Bancaria
Actualizable	Sub. Administrativa
Actualizable	Administrador de la Red

Los respaldos son realizados conforme a un calendario, elaborado por el mismo Departamento de Tecnologías cada inicio de año. La información respaldada se encuentra a disposición de las áreas responsables de la misma, mediante los mecanismos internos establecidos por el Departamento de Tecnologías.

En caso de ser necesario, la información respaldada con fecha más reciente, servirá para restablecerla en un ambiente operativo alterno.

PLAN DE MANTENIMIENTO

Como se ha mencionado en el apartado “Consideraciones y Actividades Preventivas” de este mismo documento, el Departamento de Tecnologías de la Información, ha considerado implementar sistemas redundantes en los puntos críticos de la red de servicios informáticos, con la finalidad no solamente de poder responder de manera efectiva ante una contingencia, si no también, de realizar mantenimientos preventivos y/o correctivos a estos sistemas; Siendo éstas, actividades transparentes y casi imperceptibles para el usuario.

De manera aleatoria se realizan pruebas y verificaciones de funcionalidad en el sistema de servidores de la red, y una vez al mes se hacen inspecciones de estado y funcionamiento de los equipo de cómputo instalados en las oficinas del Instituto, permitiendo actuar de manera preventiva y hacer

modificaciones a los procedimientos establecidos en este plan de contingencias.

PLAN DE ENTRENAMIENTO

El personal que participará en las etapas de antes, durante y después de la contingencia, es el que pertenece al Departamento de Tecnologías de la Información. Cada uno tiene funciones bien definidas: 1 para la coordinación, 2 para el sistema de servidores, 2 para actividades de apoyo técnico, además del personal de la oficina de Gobierno Electrónico y Desarrollo de Sistemas, para verificar la funcionalidad de los sistemas y acceso a la información electrónica.

Por lo que el personal que intervendría se encuentra preparado para atender las acciones tomadas para enfrentar la contingencia.

CONSIDERACIONES Y ACTIVIDADES PREVENTIVAS

Ante la alta responsabilidad asignada al Departamento de Tecnologías de la Información, de mantener el servicio continuo y en buen funcionamiento del aparato tecnológico informático, éste ha venido mostrando una actitud proactiva, implementando programas y actividades que coadyuven al cumplimiento de este objetivo, y a enfrentar de la mejor manera, la presencia de las contingencias.

A continuación se refieren estas actividades:

1.- *Asignación de Equipo de Cómputo.* Cada dispositivo o equipo de cómputo perteneciente al Instituto, es asignado a una persona para su cuidado y buen uso.

2.- *Energía Eléctrica Exclusiva para Equipo de Cómputo.* Se cuenta con red de alimentación eléctrica regulada y aterrizada independiente, con planta de emergencia para garantizar la calidad y continuidad en el suministro, además, cada equipo de cómputo es conectado a ella mediante un dispositivo de respaldo de energía ininterrumpible (No-Break) para soportar apagones inesperados.

3.- *Control de Acceso en las Computadoras*. Implementación de claves de encendido del equipo y de acceso a la red de cómputo, implementación de control de acceso a dispositivos de Entrada/Salida de la computadora.

4.- *Enlaces de Comunicación Principal*. Redundancia en los enlaces físicos y lógicos (fibra óptica y de cobre) que establecen la comunicación entre el sistema de servidores y los equipos de distribución de datos (IDF). También se cuenta con equipos de comunicación activa de soporte para sustitución.

5.- *Sistema de Servidores Informáticos*. Redundancia en el sistema de servidores, tanto en el sistema Windows como de Novell, para mantener en alta disponibilidad y tolerancia a fallos los Servicios y Aplicaciones Informáticas. Se cuenta también con dos servidores con sistema Windows, listos para correr de manera independiente las aplicaciones informáticas, ubicados: uno en un edificio alterno dentro de las oficinas centrales del Instituto y otro, de menores características solo para contingencias, en una oficina externa a las instalaciones pertenecientes al IPE. Con el sistema de Novell Netware, se hacen réplicas exactas de los discos duros con el sistema operativo y datos de ambos servidores.

6.- *Ambiente de Operación*. Cuarto independiente, de acceso restringido, para el sistema de servidores y comunicaciones, climatizado y con puerta de cerrado con chapa. Extintores de fuego, a una distancia de 4 metros aproximadamente para el SITE de servidores e IDF´s, luces de emergencia y detector de humo.

7.- *Políticas de Seguridad Informática*. Elaboración de un documento en donde se establece el manejo de la información electrónica Institucional, manipulación de equipo de cómputo y reglas de buena conducta.

8.- *Aseguramiento de la Información Electrónica Institucional*. Establecimiento de un modelo de respaldo-restauración de información contenida en los servidores de aplicación, en medios magneto-ópticos. Esta actividad se realiza conforme a un programa de respaldos, elaborado por el Departamento de Tecnologías de la Información.

9.- *Aseguramiento de Software Comercial Adquirido por el Instituto*. Realización de copias en CD/DVD para uso cotidiano del software comercial original, y resguardo de los medios originales en Caja de Seguridad del Instituto.

PLAN DE CONTINUIDAD

En esta sección se describen las actividades a realizar, por parte del personal del Departamento de Tecnología de la Información, para enfrentar la contingencia y restablecer, de manera pronta, los servicios de red informáticos.

Las actividades se presentan en forma enumerada y estructura, considerando dos circunstancias o escenarios:

Escenario 1: Con acceso a las instalaciones del IPE.

Escenario 2: Sin posibilidad alguna de acceso a las instalaciones del IPE.

Escenario 1.

1.Evaluar el daño.
2.Enterar a la Dirección General del IPE y al área o áreas afectadas de la magnitud del daño, la estrategia a seguir y el tiempo estimado de rehabilitación del o los servicios.
3.Utilizar equipo o material de soporte para sustituir al dañado.
4.En caso de no contar con equipo o material para sustitución, tomar la decisión de utilizar equipo en funciones de otra área para abastecer la parte o sector dañado, previa evaluación de afectación del servicio en esa área, o reubicar físicamente a usuarios con actividades prioritarias en espacios alternos, mientras éste sea adquirido, en cualquiera de sus formas: Compra, renta o préstamo.
5.De ser necesario, solicitar el apoyo según lo requerido, de los servicios de otra área del Instituto o empresa externa especializada.
6.Después de habilitar nuevamente los servicios de la red de datos, informar a la Dirección General de este Instituto y a la o las áreas afectadas de las condiciones en que se estará otorgando el servicio.

Escenario 2.

1. Esperar a recibir instrucciones por parte de la dirección general.
2. Obtener el respaldo más reciente a la fecha, de la información electrónica respaldada, resguardada en la caja de seguridad de la Institución bancaria.
3. Acudir a la oficina externa, en donde se encuentra alojado el servidor de aplicaciones alterno, con sistema Windows, y restaurar la información electrónica Institucional obtenida.
4. Adquirir en cualesquiera de sus formas: Compra, renta o préstamo; máquinas computadoras e impresoras, en número, de acuerdo a las instrucciones emitidas por la Dirección General, considerando que se utilizarán solo para procesos prioritarios y por el tiempo que dure la contingencia.
5. De ser necesario, instalar con el disco replica, el servidor con el sistema operativo de Novell Netware denominado “IPE”.
6. Realizar respaldos diarios de la información electrónica manejada en el o los servidores, para su aseguramiento y posterior restauración.
7. Una vez terminada la contingencia, recibir instrucciones por parte de la Dirección General del IPE, para conocer las condiciones y actividades para el restablecimiento de los servicios de red Informática.