SUBDIRECCIÓN DE ADMINISTRACIÓN

DEPARTAMENTO DE INFORMÁTICA

Plan de Contingencia

El objetivo del Plan de Contingencia es proporcionar la continuidad y recuperación de los servicios de Tecnologías de la Información y Comunicaciones en previsión de algún evento crítico. De acuerdo a las necesidades del Instituto Nacional de Geriatría "INGER".

Actividades Asociadas

Las actividades consideradas en este documento son:

1. Análisis de Riesgos
2. Medidas Preventivas
3. Previsión de Desastres Naturales
4. Plan de Recuperación
5. Acciones de Recuperación
6. Consideraciones adicionales

1. Análisis de Riesgos

En lo que respecta a los riesgos relacionados con las Tecnologías de la Información y Comunicaciones del INGER, se pueden identificar los siguientes riesgos:

- Falla en comunicación a Internet.
- Falla en comunicación de voz.
- Falla en hardware y/o software de servidores.
- Falla en aplicaciones.
- Virus.

1.1. Bienes susceptibles de un daño

Se puede identificar los siguientes bienes afectos a riesgos:

Infraestructura:

a) Hardware (equipos de cómputo de escritorio, portátiles, impresoras, multifuncionales, routers, switchs, etc.)

Información:

a) Datos

b) Software

1.2. Daños

Los posibles daños pueden referirse a:

a) Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes, sea por causas naturales o humanas.
b) Imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas, sean estos por cambios involuntarios o intencionales, por ejemplo, cambios de claves de acceso, eliminación de información, etc.

1.3. Prioridades

La estimación de los daños en los bienes y su impacto, fija una prioridad en relación a la cantidad del tiempo y los recursos necesarios para la reposición de los servicios que se pierden en el acontecimiento.

Riesgos	Impactos	Criticidad	Tiempo de Recuperación
Falla en infraestructura	1. Enlace de Internet sin comunicación: • Usuarios internos sin acceso a Internet • Usuarios externos sin acceso a la página del Instituto.	 Alta Alta	 1 hora
	2. Problemas en equipos con funciones de servidor, sin acceso a: • Páginas web Institucional, Biblioteca Virtual, Educación a distancia. • Dominio • Intranet	 Alta Media Baja	 1 hora
	3. Falla técnica en líneas telefónicas • Sin comunicación telefónica externa.	 Alta	 24 horas
Virus Informático	1. Virus Informático • Pérdida de datos • Saturación de red • Daño en sistema operativo de equipos de cómputo	 Alta Alta Alta	 4 horas

1.4. Fuentes de daño

Las posibles fuentes de daño que pueden causar la no operación normal asociadas al Departamento de Informática son:

Desastres Naturales

a) Movimientos telúricos que afecten directa o indirectamente a las instalaciones físicas de soporte (edificios) y/o de operación (equipos computacionales).

Falla en infraestructura

a) Inundaciones causadas por falla en los suministros de agua.
b) Falla en equipos con funciones de servidor (aplicaciones y datos), tanto en su(s) discos(s) duro(s) como en procesadores.
c) Falla en cableado de red
d) Fallas en los equipos de soporte:
-Por fallas de la red de energía eléctrica pública por diferentes razones ajenas al Instituto.
-Por falta de equipo de control de ambiente (aire acondicionado en Site e IDF'S).
-Por fallas en los servicios de voz y datos por parte de los proveedores del servicio.

Falla por Hackeo

Intromisión no calificada a procesos y/o datos de los sistemas.

Falla por Virus Informático

Instalación de software de comportamiento errático y/o dañino para la operación de los Sistemas computacionales en uso.

Falla de Software

Falla en el sistema operativo o cualquier software instalado en los equipos con funciones de servidores.

Fallas del Personal Clave

Se considera personal clave aquel que cumple una función vital en el flujo de procesamiento de datos u operación de los Sistemas de Información:

a) Personal de Informática.

Pudiendo existir los siguientes inconvenientes:

a) Enfermedad.

b) Accidentes.

c) Renuncias.

Proveedores con Fallas Técnicas

Servicios contratados con terceros, con ocurrencia de fallas por diferentes razones ajenas al manejo por parte del Instituto.

2. Medidas Preventivas

2.1. Control de Accesos

a) Acceso físico de personas no autorizadas.

El acceso físico a los diferentes sitios que se encuentran en el INGER se encuentran restringidos por puertas con seguridad (cerradura especial), a las cuales solo el personal del Departamento de Informática tiene acceso, esto con la finalidad de evitar cualquier fallo ocasionado por personal ajeno a ésta.

b) Acceso a la Red de PC's y Servidor.

Tanto el acceso a red de pc's y servidores, se encuentra controlado por un controlador de dominio el cual determinará los equipos pertenecientes a la red; así como usuarios y contraseñas, brindando diferentes niveles de seguridad.

2.2. Respaldos

Como parte importante de un Plan de Contingencia Informático se encuentra el Procedimiento de Respaldo (Manual de procedimientos del INGER), el cual nos permite conocer el proceso para la generación de los diferentes respaldos y nos proporcionará la medida de la pérdida de información relevante para dar continuidad a la operación del trabajo institucional.

3. Previsión de desastres Naturales

La previsión de desastres sólo se puede hacer bajo el punto de vista de minimizar los riesgos innecesarios en el site (cuarto de servidores), cuarto de comunicaciones, etc., en la medida de ubicación correcta del equipo ante un sismo que pueda generar mediante su caída y/o destrucción, la interrupción del proceso de operación normal, así como el de respaldo, al tener claro los lugares de resguardo, vías de escape y de las ubicaciones de los archivos y discos de respaldo del Instituto.

3.1 Adecuado Soporte de Utilitarios

Las fallas de los equipos de procesamiento de información pueden minimizarse mediante el uso de otros equipos, a los cuales también se les debe controlar periódicamente su buen funcionamiento, nos referimos:

a) Unidades de Respaldo de Energía en: equipos de cómputo, equipos con funciones de servidor, router, switch, etc.

3.2 Seguridad Física del Personal

Como medida de seguridad física del personal, se deberán seguir las establecidas por la unidad de protección civil del INGER.

3.3 Seguridad de la Información

Esta parte refiere al acceso a información contenida en los diversos sistemas, la cual deberá está protegida por claves de acceso; así como un adecuado seguimiento al plan de respaldo.

4. Plan de Recuperación

4.1 Objetivos del Plan de Recuperación

Los objetivos del plan de Recuperación son:

1. Determinación de los procedimientos de respaldos de información.
2. Reactivación de la operación interrumpida producida por un desastre de los sistemas prioritarios.
3. Permanente mantenimiento y supervisión de los sistemas y aplicaciones.
4. Establecimiento de una disciplina de acciones a realizar para garantizar una rápida y oportuna respuesta frente a un desastre (Plan de Continuidad de Operaciones del INGER).

4.2 Alcance del Plan de Recuperación

El objetivo es restablecer en el menor tiempo posible el nivel de operación normal de los equipos de cómputo y telecomunicaciones, basándose en los planes de emergencia y de respaldo.

4.3 Activación del Plan

Decisión

Queda a juicio de la Dirección General y la Subdirección de Administración determinar la activación del Plan de Contingencia.

Duración estimada

Dependiendo de la situación, se determinará la duración estimada de la interrupción del servicio.

Responsables

- Orden de Ejecución del Plan – Dirección General
- Supervisión General del Plan – Subdirección de Administración
- Supervisión del Plan de Recuperación – Departamento de Informática
- Tareas de Recuperación – Personal de tareas afines

Aplicación del Plan

El plan se aplicará en caso de que se suspenda el servicio por más de 24 hrs.

5. Acciones de recuperación

Las acciones de recuperación serán diseñadas para cada uno de los impactos mostrados anteriormente, definiendo asimismo los responsables de dichas actividades.

5.1 Falla en Comunicación a Internet

Acciones	Responsabilidad
Sin conexión a internet Verificar equipos de telecomunicaciones, levantar reporte con el proveedor del servicio (TESECOM/AXTEL). Dar seguimiento al reporte para su rápida restauración.	Departamento de Informática

5.2. Falla en Comunicación de voz

Acciones	Responsabilidad
Falla de en líneas telefónicas En caso de falla en el servicio de telefonía, levantar el reporte correspondiente con el proveedor (Telmex). Dar seguimiento al reporte para su rápida restauración.	Departamento de Informática

5.4 Virus Informático

Acciones	Responsabilidad
Pérdida de datos En caso de pérdida de datos en equipos de cómputo de los usuarios, se procede a levantar el reporte respectivo, se canaliza reporte a Eknology Solutions (proveedor de equipo y soporte) para posible recuperación de la información afectada.	Departamento de Informática
Saturación de la red Si el virus informático está saturando la red, se realizará un monitoreo, con el fin de localizar el origen del tráfico excesivo y eliminar la causa del problema.	TESECOM/Departamento de Informática

Daño en software de equipos de cómputo Reinstalar el software dañado.	Departamento de Informática

6. Consideraciones Adicionales

- La Subdirección de Administración deberá de tener una lista de contratos y proveedores que brinden algún servicio que esté identificado como prioritario.