



VERACRUZ
GOBIERNO
DEL ESTADO



SS
Secretaría
de Salud

CODAMEVER
Comisión de Arbitraje
Médico del Estado
de Veracruz



ME LLENA DE ORGULLO

PLAN DE CONTINGENCIAS

1824 Y 2024

RECUPERACION DE DESASTRES

DE LA

COMISIÓN DE ARBITRAJE MÉDICO

DEL

ESTADO DE VERACRUZ

2024: 200 AÑOS DE VERACRUZ DE IGNACIO DE LA LLAVE COMO PARTE DE LA FEDERACIÓN 1824-2024

Av. Héroes de Puebla 660 esq. Simón Bolívar.
Col. Ignacio Zaragoza
C.P. 91910, Veracruz, Ver
Tel. 229 934 0444
LADA: 800-714-7658
www.codamedver.gob.mx



200 AÑOS
VERACRUZ
DE IGNACIO DE LA LLAVE
COMO PARTE DE LA FEDERACIÓN



FIRMAS DE AUTORIZACIÓN

ELABORÓ

REVISÓ



OSCAR DAVID GUTIÉRREZ ALAMILLO
ANALISTA DE INFORMÁTICA



LIC. GUILLERMO BELLO RAMOS
SUBDIRECTOR ADMINISTRATIVO

AUTORIZÓ



DRA. ANGÉLICA SERRANO ROMERO
COMISIONADA



ÍNDICE

INTRODUCCIÓN

OBJETIVO

ALCANCE

ORGANO RESPONSABLE

MARCO DE REFERENCIA

DEFINICIONES DE TÉRMINOS EMPLEADOS

ESCENARIOS DE CONTINGENCIA

ETAPAS DEL PLAN

RECURSOS

ANÁLISIS DE RIESGOS

FALLA DE EQUIPO DE COMUNICACIÓN (Tipo de Impacto Alto)

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

ATAQUE DE VIRUS INFORMÁTICO (Tipo de Impacto Medio)

FALLAS DE ENERGÍA ELÉCTRICA (Tipo de Impacto Alto)

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

PLAN DE RESPALDOS

PLAN DE MANTENIMIENTO

CONSIDERACIONES Y ACTIVIDADES PREVENTIVAS

PLAN DE CONTINUIDAD

INTRODUCCIÓN

La Comisión de Arbitraje Médico del Estado de Veracruz, 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 la Comisión 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 equipos informáticos.

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 de la Comisión de Arbitraje Médico del Estado de Veracruz, el cual permita restaurar los servicios de la red de cómputo de forma rápida y eficiente.

ALCANCE

Este Plan contempla el actuar del personal de la Oficina de Recursos Materiales y Tecnologías de la Información, ante la presencia de una contingencia, en las oficinas de la Comisión de Arbitraje Médico del Estado de Veracruz. Ubicado en la Av. Héroes de Puebla #660 esq. Simón Bolívar, Col. Ignacio Zaragoza en la ciudad de Veracruz, Ver.

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

ORGANO RESPONSABLE

Oficina de Recursos Materiales y Tecnologías de la Información, adscrito a la Subdirección Administrativa.

MARCO DE REFERENCIA

La Comisión de Arbitraje Médico del Estado de Veracruz cuenta con una red de datos instalada en sus oficinas con cableado estructurado categoría 6 constituido con cable de cobre UTP y fibra óptica, red de energía eléctrica regulada exclusiva para equipos de cómputo, oficinas con equipos de cómputo: Computadoras, Impresoras, Multifuncionales, Escáneres, Equipos de comunicación, etc.

En el 3er piso del edificio está ubicado el cuarto principal de comunicaciones. En él se encuentra instalado un rack con un Conmutador Híbrido Inteligente Mod. KX-NS500 de la marca Panasonic y su respectivo panel de parcheo administrado por dos Switches TP-Link Mod. TPL-SG1024 de 24 puertos. También se encuentran 2 Módems de Telmex fibra óptica y uno de Megacable igualmente de fibra óptica, los cuales dan servicio de internet vía cableado Ethernet e inalámbrico.

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 de la Comisión por diversas causas: Políticas, Organizacionales, Siniestro, etc.
- 3.- La pérdida parcial o total, del área donde se encuentra ubicado el SITE de comunicaciones.
- 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 Continuidad

RECURSOS

HUMANOS

-Personal del Departamento de Tecnologías de la Información.

TÉCNICOS

- Switches de 48 puertos., Velocidad 10/100 o mayor de preferencia.
- Equipo de respaldo de energía eléctrica (No break) con capacidad de 750 watts o mayor.
- Servidor de Aplicaciones con capacidad para soportar sistema operativo de red Windows Server 2008 y manejador de base de datos.
- Computadora de escritorio con sistema operativo Windows 8.1 o Superior.
- 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
Acceso a la Red No Autorizado	Alto
Ataque de Virus Informático	Medio
Fallas de Energía Eléctrica	Alto
Imposibilidad de acceso a las instalaciones (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 Wi-Fi 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.

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 y sistemas de información.
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)

La Comisión cuenta con el software de seguridad antivirus, para 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 servicios de red e internet, para los casos de corte de energía y determinar el tiempo que queda de energía auxiliar.
2. Llamar a las Oficinas de la Comisión Federal de Electricidad 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 servicios de comunicación y desconectarlo de la toma corriente.
4. Realizar los avisos pertinentes a los usuarios de todos los departamentos, para hacerles de su conocimiento del fenómeno presentado.
5. Esperar el aviso por parte de la Comisión Federal de Electricidad para reanudar el servicio de red e internet.
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 (SINIESTRO NATURAL) (Tipo de Impacto Alto)

La ocurrencia de ambos eventos tendría como consecuencia el No acceso, total o parcial, a las oficinas de la Comisión 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 equipos de cómputo de los usuarios, consiste en realizarlo cada fin de mes en todos los departamentos.

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 la Oficina de Recursos Materiales y Tecnologías de la información.

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, la Oficina de Recursos Materiales y 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 comunicaciones, y una vez al mes se hacen inspecciones de estado y funcionamiento de los equipo de cómputo instalados en las oficinas de la Comisión, permitiendo actuar de manera preventiva y hacer modificaciones a los procedimientos establecidos en este plan de contingencias.

CONSIDERACIONES Y ACTIVIDADES PREVENTIVAS

Ante la alta responsabilidad asignada a la Oficina de Recursos Materiales y 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 a la Comisión, 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 para garantizar la calidad 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. Ambiente de Operación. Oficina de acceso restringido, para el sistema de comunicaciones, climatizado. Extintor de fuego, a una distancia de 4 metros aproximadamente para el SITE de comunicaciones.
4. 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.
5. Aseguramiento de la Información Electrónica Institucional.
6. Establecimiento de un modelo de respaldo-restauración de información contenida en los equipos de los usuarios, en medios magneto-ópticos y electrónicos. Esta actividad se realiza conforme a un programa de respaldos, elaborado por el Departamento de Tecnologías de la Información.
7. Aseguramiento de Software Comercial Adquirido por la Comisión.
8. Realización de copias en CD/DVD para uso cotidiano del software comercial original, y resguardo de los medios originales en las oficinas administrativas.

PLAN DE CONTINUIDAD

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

2024: 200 AÑOS DE VERACRUZ DE IGNACIO DE LA LLAVE COMO PARTE DE LA FEDERACIÓN 1824-2024

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

ESCENARIO 1: Con acceso a las instalaciones de la Comisión de Arbitraje Médico.

ESCENARIO 2: Sin posibilidad alguna de acceso a las instalaciones de la Comisión de Arbitraje Médico.

ESCENARIO 1.

1. Evaluar el daño.
2. Enterar al Comisionado, Subdirección Administrativa y jefes de departamentos de la magnitud del daño, la estrategia a seguir y el tiempo estimado de rehabilitación de los servicios afectados.
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 o departamento 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 una empresa externa especializada.
6. Después de habilitar nuevamente los servicios de la red de datos, informar al Comisionado y Jefes de Departamentos de las áreas afectadas, de las condiciones en que se estará reanudando el servicio.

ESCENARIO 2.

1. Esperar a recibir instrucciones por parte de la subdirección Administrativa y del Comisionado.
2. Obtener el respaldo más reciente a la fecha, de la información electrónica respaldada, resguardada en el medio de almacenamiento de respaldos de cada área.
3. Adquirir en cualesquiera de sus formas: Compra, renta o préstamo; máquinas computadoras e impresoras, en número, de acuerdo a las instrucciones emitidas por el Comisionado, considerando que se utilizarán solo para procesos prioritarios y por el tiempo que dure la contingencia.
4. Realizar respaldos diarios de la información electrónica manejada en los equipos, para su aseguramiento y posterior restauración.
5. Una vez terminada la contingencia, recibir instrucciones por parte de la Subdirección Administrativa y del Comisionado, para conocer las condiciones y actividades para el restablecimiento de los servicios de la red Informática.