

INDICE

Plan de Contingencia Informático

INTRODUCCION

Objetivos	4
Definiciones	5
Responsabilidades	6
Análisis y Valoración de Riesgos	7
Medidas Preventivas y Evaluación de Riesgos	9
Previsión de Desastres naturales y Jerarquización de Aplicaciones	11
Plan de Respaldo y Establecimiento de Requerimiento de Recuperación.	13
Conclusión	15

PLAN DE CONTINGENCIA INFORMÁTICO

Un **plan de contingencias** informático es una metodología para la gestión de un buen manejo y administración de las Tecnologías de la Información y las Comunicaciones (TIC'S) para tener un pleno dominio del soporte y el desempeño de la Infraestructura Tecnológica de la Academia Veracruzana de las Lenguas Indígenas.

Este plan debe tener las **medidas técnicas, humanas y organizativas** necesarias para garantizar la continuidad de las actividades de la institución. El plan se diseña para que en el caso de un siniestro se active el plan de contingencia informático permitiendo dar continuidad a las actividades de la institución, este debe ser aplicado por la Sección de Tecnología de la Información, no obstante, dada la importancia de las tecnologías, el plan de contingencias es el más relevante.

Para la elaboración de Plan de Contingencia se deben considerar: Análisis y valoración de riesgo, medidas preventivas, previsión de desastres naturales, plan de respaldo y plan de recuperación.

Existen planes de contingencia ya definidos como son: el conocido ciclo de vida iterativo PDCA (plan-do-check-act, es decir, planificar-hacer-comprobar-actuar).

La Academia Veracruzana de Lenguas Indígenas, en un momento dado, entraría en situación de contingencia 1 hora después de que sale del servicio habitual y se restablece en cuanto el procesamiento regresa a sus actividades normales.

INTRODUCCION

En este documento se presenta el Plan de Contingencia Informático de la Academia Veracruzana de las Lenguas Indígenas en materia de riesgos de tecnologías de la Información (TIC,s);

Este plan establece el objetivo, alcance y metodología desarrollada, incluye además, las definiciones utilizadas como son:

Análisis y valoración de riesgos.- Se identifican las preocupaciones y prioridades que deberá asumir la AVELI, se identificara el impacto de las afectaciones y se proporcionaran las bases de una estrategia para la contingencia operativa.

Medidas preventivas y evaluación.- Definiremos que medidas efectivas debemos tomar para controlar los diferentes accesos a los activos computaciones, consideraremos que actividades realizar para los resguardos de la información tanto operacional como financiera.

Previsión de desastres naturales y jerarquización de aplicaciones.- Aunque un desastre natural es inevitable, si podemos estar preparados, aminorar las repercusiones y tener una pronta recuperación después del desastre, y para definir lo verdaderamente importante se deben jerarquizar las aplicaciones.

Plan de respaldo y establecimiento de requerimientos de recuperación.- Después de haber desarrollado los puntos anteriores se profundizará el siniestro y se determinará para que se de como consecuencia el modo de recuperación.

La Academia Veracruzana de las Lenguas Indígenas es un Organismo Público Descentralizado, su infraestructura es pequeña, por esta razón es que varias contingencias pueden ser resueltas a brevedad, siempre y cuando los factores no dependan del exterior.

La metodología práctica comprende: La identificación de riesgos, calificación de la probabilidad de que ocurra un riesgo, evaluación del impacto en los procesos críticos y la creación de estrategias de contingencias. Permite mantener la contingencia operativa frente a eventos críticos de la Entidad y minimizar el impacto negativo sobre la misma, los usuarios deben ser parte integral del Plan de Contingencia Informática para evitar interrupciones, estar preparados para fallas potenciales y guiar hacia una solución.

OBJETIVOS

Se deben definir las actividades de planeación, preparación, capacitación y ejecución de tareas destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.

Establecer un plan de recuperación, formación de equipos y entrenamiento para restablecer la operatividad del sistema en el menor tiempo posible.

Establecer actividades que permitan evaluar los resultados y retroalimentación del plan general.

DEFINICIONES

A. CONTINGENCIA:

Interrupción, no planificada, de la disponibilidad de recursos informáticos.

B. PLAN DE CONTINGENCIA:

Conjunto de medidas (de DETECCIÓN y de REACCIÓN) a poner en marcha ante la Presentación de una contingencia.

El Plan de Contingencia se subdivide en:

- Plan de Emergencia
- Plan de Restauración (BACKUP)
- Plan de Recuperación

El Plan de Contingencia suele combinarse con planes de seguridad general.

Plan de Contingencia

	Emergencia	Restauración	Recuperación
Objetivo	Prevenir ante una pérdida total	Continuar con la actividad normal	Recuperación total
Actuación	Revisión inmediata de los planes de contingencia	Inmediato/corto plazo	A medio plazo
Contenido	Iniciar plan de contingencia, Evacuar, revisar la magnitud del daño,	Aplicar sistemas de recuperación y aplicación de software	Recuperación de todos los recursos
Responsabilidad Principal	AVELI	Usuarios	Sección de TI

RESPONSABILIDADES

Líder del proyecto

Responsable: Jefe del Departamento Administrativo de la AVELI.

- Dirigir el desarrollo integral del Proyecto así como verificar el cumplimiento de las actividades encargadas a cada uno de los líderes usuario.

Administrador del proyecto

Responsable: Jefe de la Sección de TI de la AVELI

- Desarrollar el plan de trabajo.
- Asignar los responsables así como las prioridades para el desarrollo de las tareas.
- Organizar el proyecto y orientar al equipo de trabajo.
- Establecer coordinaciones entre el personal de la AVELI, el Líder del Proyecto y las demás Áreas involucradas.
- Verificar y efectuar el seguimiento para que el proyecto sea expresado en documentos formales y de fácil entendimiento.
- Identificar los problemas, desarrollar las soluciones y recomendar aquellas acciones específicas.
- Controlar el avance del proyecto.
- Informar al Líder del Proyecto, los avances y ocurrencias durante el cumplimiento de las tareas de los responsables.

ANÁLISIS Y VALORACIÓN DE RIESGOS

Consistes en el análisis del Impacto de los procesos, es determinar las funciones, procesos e infraestructura de soporte que son críticos.

Para lograr el objetivo principal se definieron los siguientes objetivos específicos:

- Identificar las preocupaciones y prioridades de que deberá asumir la AVELI en el caso que exista una indisponibilidad en los sistemas informáticos producida por una contingencia.
- Identificar el tiempo máximo en el que un proceso critico de la AVELI deberá ser restaurado para su normal y eficiente continuidad.
- Identificar el impacto en las aplicaciones que soportan los procesos críticos de la AVELI.
- Proporcionar las bases de una estrategia para la contingencia operativa en caso de un desastre.

Falla que lo causa	Definición/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.	NO HAY COMUNICACIÓN ENTRE CLIENTE– SERVIDOR.
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.	FALLA DE UN SERVIDOR.
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.

<p>Falla de equipos de comunicación: SWITCH, Fibra Óptica.</p> <ul style="list-style-type: none"> • Fallas en el software de Acceso a Internet. • Perdida de comunicación con proveedores de Internet. 	<p>PERDIDA DE SERVICIO DE INTERNET</p>
<p>Incendio</p> <ul style="list-style-type: none"> • Sabotaje • Corto Circuito • Terremoto 	<p>INDISPONIBILIDAD DEL CENTRO DE COMPUTO (DESTRUCCIÓN DEL SITE DE SERVIDORES)</p>

MEDIDAS PREVENTIVAS Y EVALUCION DE RIESGOS

Se debe definir medidas efectivas para controlar los diferentes accesos a los activos computacionales, e identificar en caso de que existan

- a) Acceso físico de personas no autorizadas.
- b) Acceso a la Red de PC's y Servidor.
- c) Acceso restringido a las librerías, programas, y datos

Se considera las actividades de resguardo de la información, en busca de un proceso de recuperación con el menor costo posible para la Academia Veracruzana de las Lenguas Indígenas.

Se realizan respaldos a todos los equipos de manera semestral, estos respaldos son depositados en un disco duro externo con la finalidad de que si llegara a existe algún problema ya sea por daño físico o natural, se tenga información almacenada hasta cierta fecha.

En el caso de información financiera, se realiza respaldo cada día final de mes, después de terminar de realizar los estados financieros de la Academia Veracruzana de las Lenguas Indígenas.

Las causas más representativas que originarían cada uno de los escenarios propuestos en el Plan de Contingencias y Seguridad de la Información se presentan en el siguiente cuadro.

PRINCIPALES PROCESOS IDENTIFICADOS

Costo/Beneficio/Riesgo/impacto				
Descripción	Costo/beneficio	Riegos	Impacto en caso de suspensión	Observaciones
SERVIDOR HP	Alto	Alto	Alto	Información contables y bases de datos
www.aveli.gob.mx	Medio	Bajo	Bajo	Se encuentra alojado en la SEFIPLAN
www.aveligob.mx	Medio	Bajo	Medio	Hosting, propio en el que radican cursos en línea.

Modem infinitum1	Alto	Bajo	Alto	Propiedad de TELMEX
Modem infinitum2	Alto	Bajo	Alto	Propiedad de TELMEX
Copiadora 1	Mediano	Bajo	Alto	Arrendamiento
Copiadora2	Mediano	Bajo	Alto	Arrendamiento
Disco Duro de Respaldos	Mediano	Alto	Mediano	Es un disco Externo de 3 TB
Equipos de computo Dirección general	Alto	Alto	alto	Instalar Centro de Computo Alterno
Equipo de computo Subdirección de investigación	Alto	Alto	Alto	Instalar Centro de Computo Alterno
Equipo de Telefonía Conmutador	Alto	Mediano	Alto	
Energía Eléctrica	Alto	Alto	Alto	No es parte de las TI, pero es prescindible para que funcione

PREVISIÓN DE DESASTRES NATURALES y JERARQUIZACION DE APLICACIONES

La previsión de desastres naturales sólo se puede hacer 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 considerar depositar los respaldos, o el tenerlo en lugares de resguardo, vías de escape y de la ubicación de los archivos, CD, discos con información vital de respaldo de aquellos que se encuentren aun en las instalaciones.

Los desastres causados por un evento natural o humano, pueden ocurrir, en cualquier parte, hora y lugar. Existen distintos tipos de contingencias, como por ejemplo:

- *Riesgos Naturales*: tales como mal tiempo, terremotos, etc.
- *Riesgos Tecnológicos*: tales como incendios eléctricos, fallas de energía y accidentes de transmisión y transporte.
- *Riesgos Sociales*: como actos terroristas y desordenes.

La jerarquización consiste en el orden de los elementos que integran la Academia Veracruzana de las Lenguas Indígenas en la sección de TI estos según su valor. Esta clasificación nos permitirá definir la prioridad, incluso antes de entrar un plan de contingencia intentar rescatar lo que podría generar una pérdida irreparable

Nivel	Nombre	Descripción
1	Servidor HP PROLIANT	El servidor incluye la información contable de todos los años SUAPOP 08-09-10-11-12-13-14, BD de aplicaciones, Sistema comisiones
2	Disco Duro Externo 3 TB	Información, respaldos semestrales de la academia Veracruzana de lenguas Indígenas
3	LAPTOP de la Sección de promoción editorial	Incluye material de la difusión AVELI
4	CPU Secretaria directiva	Incluye el sistema de oficios, directorio general
5	CPU de la Sección de Tecnologías de la Información.	Incluye archivos fuentes de prototipos de sistemas implementados en AVELI, sistoficios, sistpersAVELI, sistcomisionAVELI, sistinvAVELI

6	CPU Servidor administrativo	Incluye unidad X: con la información diaria del Departamento Advo. la AVELI.
7	CPU servidor Investigación	Incluye unidad T: con la información diaria de la Subdirección de Investigación.
8	CPU servidor Sub. Desarrollo	Incluye unidad R: con la información diaria de la Subdirección de Desarrollo.

PLAN DE RESPALDO Y ESTABLECIMIENTO DE REQUERIMIENTOS DE RECUPERACIÓN

Aquí profundizaremos ampliando la definición del problema determinando el tipo de siniestro, las consecuencias y el modo de recuperación.

Plan de contingencia se aplicara dependiendo del tipo del tipo de siniestro

	Clasificación	Consecuencias	Modo de Recuperación
Incendio	Grave	Dependiendo de la magnitud la gravedad será, con pérdida total del inmueble y su contenido	Respaldar y guardar en un banco de información externo, con copias constante, o adquirir un sistema de respaldo CLOUD(en la nube)
Temblor	Mediano	Dependerá de la Magnitud, pero en caso de que se desdoblé existirán equipos que soportaran y la información no será perdida en su totalidad	Respaldar y guardar en un banco de información externo, con copias constante, o adquirir un sistema de respaldo CLOUD(en la nube)
Robo	Bajo	TI, es el área que mas fácilmente sufre atracos, por ser equipos que fácilmente se pueden vender, principalmente equipos pequeños o portátiles.	Respaldar y guardar en un banco de información externo, con copias constante, o adquirir un sistema de respaldo CLOUD(en la nube)
Virus Cibernético	Medio	Dependiendo en donde caiga el virus se definirá lo daños que cause, actualmente existen SW de recuperación que rescatan en un 90% la información	En caso de pérdida. Aplicar SW correctivo que permita recuperar los archivo o cualquier documento importante que se desee recuperar
Epidemia Viral humana	Bajo	La principal perdida por este factor, es la pérdida económica, ya que se estarán pagando servicios sin ser utilizados.	

Lluvias/Huracanes	Bajo	Para estos casos afecta más a las academias regionales, que por las inclemencias de tiempo, puede provocar que la comunicación sea cortada y no envíen información o incluso hasta por impestivas lluvias	Generar respaldos constantemente en medios magnéticos y mandarlo a la oficina central.
-------------------	------	---	--

CONCLUSIÓN

El presente Plan de contingencia, tiene como objetivo el recuperar a la brevedad posible, sin tener pérdidas en los sistemas de Información, extremando las medidas de seguridad para protegernos y estar preparados a una contingencia de cualquier tipo.

Las principales actividades requeridas para la implementación del Plan de Contingencia son:

Análisis y valoración de riesgos.

Medidas preventivas y evaluación.

Previsión de desastres naturales y jerarquización de aplicaciones.

Plan de respaldo y establecimiento de requerimientos de recuperación.

El Plan de Contingencia es la herramienta que la Academia Veracruzana de las Lenguas Indígenas debe tener, para desarrollar la habilidad y los medios de sobrevivir y mantener sus operaciones, en caso de que un evento imprevisto, fuera de su alcance le pudiera ocasionar una interrupción parcial o total en sus funciones.

El plan de Contingencia de la Academia Veracruzana de las Lenguas Indígenas está sujeto a la infraestructura física y servicios que son suministrados por la Sección de Tecnologías de la Información.