UNIVERSIDAD POLITÉCNICA DEL VALLE DE MÉXICO

PLAN DE RECUPERACIÓN DE DESASTRES

Elaboró	Revisó	Aprobó
Mtro. Carlos Alberto Alba Laguna	Ing. Alexander Jonathan Olmos Marín	Dr. David Torres Franco
Jefe del Centro de Innovación Tecnológica en Informática y Comunicaciones	Jefe de Departamento de Mejora de Procesos y Calidad	Secretario Académico y Encargado del Despacho de la Rectoría

COPIA CONTROLADA

1. Objetivo

Establecer pautas que faciliten u orienten lograr una solución alternativa que permita restituir rápidamente los servicios informáticos en la Universidad Politécnica del Valle de México, ante la eventualidad de toda acción que lo pueda paralizar, ya sea se forma parcial o total.

1.1. Finalidad del Plan

- Tender a que los procesos críticos de la Universidad Politécnica del Valle de México continúen funcionando a pesar de una posible falla en los sistemas e infraestructura de TI. Es decir, un plan que permita a la Institución seguir operando aunque sea al mínimo.
- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los sistemas de información.
- Definir acciones a ejecutar en caso de fallas de los elementos que componen un sistema de información.

2. Alcance

El presente Plan de Recuperación de Desastres es de aplicación y cumplimiento obligatorio para aquellas áreas de la Universidad Politécnica del Valle de México, que administren y operen información crítica de los sistemas y aplicaciones informáticas.

3. Información documentada de referencia

- **Norma ISO 9001:2015 / NMX-CC-9001- IMNC-2015. Sistema de Gestión de la Calidad – Requisitos**
- **Ley de Gobierno Digital del Estado de México y Municipios.**
- **Reglamento de la Ley de Gobierno Digital del Estado de México y Municipios.**
- **Normas administrativas para la asignación y uso de bienes y servicios de las dependencias y organismos auxiliares del poder ejecutivo estatal.**
- **Manual General de Organización de la Universidad Politécnica del Valle de México.**

4. Responsabilidades

Responsables estratégicos: Los titulares del Centro de Innovación Tecnológica en Informática y Comunicaciones y del Departamento de Computación y Telemática.

Responsable operativo: Todo el personal que opere o administre cualquier sistema informático o que tenga bajo su resguardo equipo de cómputo o de telecomunicaciones.

5. Generalidades

Cada día es más la importancia que cobra el uso de la tecnología de información en todos los aspectos tanto laborales como personales.

Hace algunos años, cuando el proceso de la información no dependía tanto del tiempo, ni tampoco la necesidad de la información era tan dependiente en su inmediatez, era muy sencillo también establecer un plan de contingencia.

Lo único que realmente permite que una institución pueda reaccionar adecuadamente a una falla en el proceso crítico es mediante la elaboración, prueba y mantenimiento de un Plan de Recuperación de Desastres (DRP). El plan es precisamente una serie de actividades tendientes a restablecer la operación normal, en un evento de calamidad, interno o externo.

El DRP debe obedecer a un proceso formal y debe ser la conclusión de un proyecto de elaboración del mismo, que incluya la identificación de los factores críticos, el establecimiento de los equipos de trabajo y alternativas de solución de la contingencia, una prueba real del mismo plan, una capacitación de las personas involucradas y una constante actualización.

5.1. Planificación de Contingencia

El DRP de la UPVM ha sido desarrollado después de efectuar un minucioso estudio de los aspectos más importantes que intervienen en la Planificación de Desastres en áreas de TI. El Plan está orientado a establecer, junto con otros trabajos de seguridad, un adecuado sistema de seguridad física y lógica en previsión de cualquier desastre.
El presente Plan da mayor prioridad a la necesidad de contar con estrategias eficientes en el Análisis de Riesgos, de Prevención, de Emergencia, de Respaldo, de Recuperación y, finalmente, de Costos para planificar y enfrentar desastres.

5.2. Actividades

Las actividades consideradas en este Plan, son las siguientes:

- EL ANÁLISIS DE RIESGO, cuyo objetivo es el de identificar los bienes de la Institución, asignarle sus respectivos costos y determinar el costo/beneficio de las medidas de seguridad;
- LAS MEDIDAS PREVENTIVAS, que permitirán reducir las exposiciones a los riesgos;
- LAS ESTRATEGIAS DE EMERGENCIA, que intentan reducir el daño que provocan los desastres y mantener el servicio a usuarios finales;
- EL PLAN DE RESPALDO, que contempla el desarrollo y cumplimiento de procedimientos críticos de la función, entre el desastre y la recuperación; y
- EL PLAN DE RECUPERACIÓN, que prevé el pronto restablecimiento de los servicios después de un desastre.

6. Análisis de Riesgos

6.1. Estimación de Daños Potenciales

Esta será la primera actividad a realizar dentro del Análisis de Riesgos. En esta actividad se realizarán las siguientes tareas:

- Identificación de los bienes de la UPVM pertenecientes al rubro Tecnología de Información (T.I.).
- Identificación de las características de los bienes.
- Identificación de los posibles daños a los que los bienes pudieran estar expuestos.
- Establecimiento de un criterio de asignación de valores (probabilidad de ocurrencia, impactos, costos) y prioridad a las tareas y aplicaciones.
- Identificación de las tareas y aplicaciones críticas.

6.2. Bienes

Se considerarán las siguientes categorías de bienes, el tiempo que requiere reemplazarlos y las aplicaciones específicas sobre las cuales puedan causar impactos:

- Personal.
- Hardware.
- Equipos de telecomunicaciones.
- Software.
- Datos e información.
- Documentación.
- Suministro de energía eléctrica.

6.3. Daños

El término "daños" puede referirse a:
Negación de recursos:

- Daños estructurales de los edificios por desastres naturales.
- Tomas de instalaciones y prohibición de ingreso a los edificios.
- Sabotaje a alguna de las instalaciones.

Modificación del sistema instalado:

- Cambios en las claves de ingreso.
- Cambios de códigos de datos importantes.
- Cambios de datos personales.
- Borrado o eliminación de información.
- Ejecución de procesos no deseados.
-

Revelación de información:

- Robo de información.
- Introducción de información no fiable.

6.4. Prioridades

La primera fase de la estimación de daños potenciales ha sido la de identificar los bienes prioritarios de tal manera que, con correcta protección y respaldo, pueda garantizarse la continuidad del servicio.

7. Análisis de Amenazas

Se ha determinado que, efectivamente, existen amenazas que podrían afectar la operación normal de la infraestructura de T.I. de la UPVM, y causar serios problemas, incluso a los sistemas de información. Se han definido como posibles amenazas a las siguientes:

- Acceso no autorizado.
- Desastres naturales.
- Proximidad de peligros.
- Fallas en los equipos de soporte.
- Indisponibilidad de personal clave.
- Fallas de hardware.
- Incendios.

8. Medidas Preventivas

En conjunción con el Análisis de Riesgos, se deberán establecer las siguientes medidas preventivas a fin de reducir la exposición al riesgo:

8.1. Rigurosidad en el Control de Accesos

- Acceso físico de personas no autorizadas.
- Acceso a los sistemas

8.2. Previsión para Desastres Naturales

Siendo los desastres naturales los más difíciles de predecir y controlar, las amenazas se reducirán significativamente con un adecuado entrenamiento del personal, el cual deberá saber cómo actuar principalmente en casos de temblores o terremotos. El personal involucrado en la seguridad de T.I. será capaz de ubicar los archivos, discos y cualquier otro dispositivo de almacenamiento, en caso de existir, con información vital.

8.3. Evitando la Proximidad de Peligros

Todo el personal será debidamente instruido para estar en capacidad de identificar personas, paquetes y vehículos sospechosos alrededor de las instalaciones para reportarlos al personal de seguridad o a las autoridades correspondientes.

8.4. Adecuado Soporte a los Equipos e Instalaciones

En el caso de corte de energía eléctrica, se cuenta con plantas generadoras, además de tener equipos UPS en los equipos que soportan la conectividad de voz y datos, así como en los servidores de misión crítica. Se deberá proporcionar un adecuado mantenimiento a estos equipos.

Para evitar falla de los equipos de telecomunicaciones que soportan los servicios, se gestionará la contratación de pólizas de garantía y mantenimiento, que permitan la atención por parte del fabricante o del proveedor.

En cuanto a los servicios que proporciona el proveedor de Internet y de telefonía, las empresas proveedoras se comprometen a reestablecer lo más pronto posible en caso de contingencia.

8.5. Seguridad de la Información

La información generada con las aplicaciones de sistemas informáticos, será cuidadosamente protegida en doble respaldo. El primer respaldo será almacenado en el site principal (Edifico A) y el segundo (copia) será almacenado en el edificio F. Adicionalmente se analizará la contratación de servicios en la nube, que permita mantener un tercer respaldo fuera de las instalaciones de la UPVM.

8.6. Seguridad de la Documentación

La documentación se considera en este Plan tan importante como los datos e información misma. Como medida preventiva, se analiza el proyecto de digitalización de la documentación generada en las áreas.

8.7. Confiabilidad de Hardware y Software Instalado

A fin de garantizar un adecuado nivel se servicio y reducir al mínimo los desastres que podrían derivarse de una falla de hardware, se deben realizar el mantenimiento periódico en los siguientes equipos:

- Sistemas de energía ininterrumpida (UPS) del site principal.
- Switch principal de la red.
- Equipo de seguridad perimetral - firewall (a través del proveedor de internet).
- Sistema de telefonía IP.
- Cuartos de telecomunicaciones
- Servidores que soportan el sistema SIIPPEA.

Además, la información publicada en la página web se tiene hospedada en servidores del Gobierno del Estado de México.
Referente a software, se promueve la separación del ambiente de producción de los sistemas del ambiente de desarrollo y programación. Además, los servidores de aplicaciones cuentan con software antivirus.

9. Definiciones y siglas.

Concepto	Descripción
DRP	Plan de Recuperación de Desastres
Firewall	Cortafuegos
TI	Tecnologías de la Información
TIC	Tecnologías de la Información y Comunicaciones
UPS	Sistema de energía ininterrumpida
UPVM	Universidad Politécnica del Valle de México

10. Control de cambios.

Revisión	Fecha de registro en Lista maestra de Control de Cambios	Responsable