UJED
Universidad Juárez
del Estado de Durango

PLAN DE CONTINGENCIA Y RECUPERACION EN CASO DE DESASTRES

DIRECCIÓN DE TRANSFORMACIÓN DIGITAL

Introducción

En la actualidad los cambios tecnológicos adquieren cada vez mayor importancia al interior de las organizaciones, no menos importante es también el cuidado de la integridad del recurso humano, por lo cual se hace necesario o indispensable contar con un plan de contingencias, que garantice el restablecimiento del correcto funcionamiento de los servicios en el menor tiempo posible, ante cualquier eventualidad.

Propósito

El propósito de este plan es mantener la continua ejecución de los procesos de misión crítica y sistemas de información tecnológica de la UJED en el caso extraordinario que un evento pudiera ocasionar que los sistemas fallen en el mínimo de su producción. El Plan de Contingencia de la UJED contiene las necesidades y requerimientos de tal forma que la institución pueda estar preparada para responder a un evento y, en su caso, hacer eficiente la restauración de los sistemas que hayan estado inoperables por el evento.

Objetivo

Proporcionar a la UJED una herramienta que le permita garantizar el funcionamiento de la tecnología informática y la recuperación en el menor tiempo posible de cualquier falla que interrumpa el servicio.

Las medidas principales son mantener la conectividad, acceso a internet, correo electrónico u otras aplicaciones institucionales críticas para la operación como desarrollos propios de sistemas de bases de datos.

El plan busca los siguientes objetivos:

- Minimizar el número de decisiones que deben ser tomadas durante una contingencia
- Identificar los recursos necesarios para ejecutar las acciones definidas.
- Identificar información critica, así como el responsable de recuperarla en las operaciones de restauración
- Definir el proceso para probar y mantener este plan y entrenamiento para equipos de contingencia de la organización.

Sistemas/aplicaciones/servicios de misión critica

Los siguientes sistemas/aplicaciones/servicios de misión crítica deberán ser recuperados en el caso de un desastre:

Área	Acrónimo del Sistema	Nombre Sistema
Redes	*Conectividad LAN*	*Conexión de Red Interna*
Redes	*Conectividad WAN*	*Conexión de Red Externa*
Redes	*Servicio de Telefonía*	*Conexión Interna y al Proveedor*
Servidores	DNS	Servicio de Resolución de Nombres
Servidores	Maquinas Virtuales	Portales y Sistemas Institucionales
Sistemas	BD	Base de Datos Institucional

Amenazas

La siguiente tabla muestra las amenazas más comunes que podrían impactar la continuidad y componentes de sistemas y su administración.

Probabilidad de Amenazas			
Probabilidad de Ocurrencia:	Alta	Media	Baja
Falla física en Servidores y/o equipo de Telecomunicaciones		*X*	
Falla del aire acondicionado		*X*	
Amenazas de bomba			*X*
Frío / helada / Nieve		*X*	
Perdida de comunicación		*X*	
Destrucción de información		*X*	
Fuego		*X*	

Inundación / Daño por agua			*X*
Corte eléctrico / Interrupción	*X*		
Sabotaje / Terrorismo			*X*
Vandalismo		*X*	
Tormentas / Huracanes		*X*	

Plan de contingencia para el suministro de energía eléctrica en el SITE principal de la UJED

Acciones Preventivas a la Contingencia

Planta de Emergencia

Acción	Frecuencia	Responsable
Supervisar el nivel óptimo de combustible, agua, baterías, etc.	Semanal	Dpto. Infraestructura
Mantenimiento Preventivo Menor	Mensual	Dpto. Infraestructura
Mantenimiento Preventivo Mayor	Anual	Proveedor externo
Contar con números de contacto de proveedor en caso de fallas	NA	Dpto. Infraestructura

UPS

Acción	Frecuencia	Responsable
Revisar que la carga del mismo no sea superior al 80% de la capacidad.	Semestral	Dpto. Infraestructura
Mantenimiento Preventivo Mayor	2 años	Proveedor externo

Realizar el cambio de Baterías según especificación fabricante	(Entre 3 y 4 años)	Dpto. Infraestructura
Contar con números de contacto de proveedor en caso de fallas	NA	Dpto. Infraestructura

Acciones Durante la Contingencia

En caso de interrupción del suministro eléctrico

Paso	Acción
1	Revisar que la planta de emergencia entre en operación.
2	Revisar el estado de carga de los UPS
3	En caso de que el problema sea externo levantar reporte con CFE
4	En caso de que el problema eléctrico sea Interno reportar a Servicios Generales
5	Apagar equipos no prioritarios para disminuir consumo de energía
6	Mientras no regrese el suministro eléctrico revisar en periodos de 1 hora, el nivel de combustible y estado de la planta así como de los UPSs.
7	En caso de prolongarse por más 3 horas dar aviso a usuarios prioritarios así como reabastecer el combustible.

Acciones Después la Contingencia

Paso	Acción
1	Brindar tiempo de gracia para reestablecer equipos y/o servicios que se apagaron
2	Revisar el estado de carga de los UPS así como niveles de la planta para reponer combustible consumido.
3	Validación de servicios, portales y sistemas

Plan de contingencia para daño físico de servidores y/o equipo de Telecomunicaciones

Acciones Preventivas a la Contingencia

Servidores

Acción	Frecuencia	Responsable
Respaldo de Información a nivel de máquina virtual (VM)	Aumátizada de 1 a 3 días dependiendo de lo crítico del servicio	Dpto. Infraestructura
Revisión del estado de arreglos de discos en servidores (RAID)	Mensual	Dpto. Infraestructura
Revisión de la integridad de la máquina virtual (VM) a nivel de ficheros	Mensual	Dpto. Infraestructura
Mantenimiento preventivo a los equipos	Anual	Dpto. Infraestructura
Revisión de la temperatura de operación de los servidores	Diario	Dpto. Infraestructura

Equipo de Telecomunicaciones

Acción	Frecuencia	Responsable
Respaldo de archivos de configuración de los equipos principales	Automatizado al generar cambios de configuración	Dpto. Infraestructura
Monitoreo de estado de operación de los equipos (Uso de CPU, conectividad, uso de ancho de banda)	Semanal	Dpto. Infraestructura

Mantener actualizada documentación de direccionamiento	Actualizar cada vez que se realicen modificaciones	Dpto. Infraestructura
Revisar enlaces redundantes en los sitios principales	Mensualmente	Dpto. Infraestructura
Contar equipo en bodega para remplazo		Dpto. Infraestructura

Acciones Durante la Contingencia

En caso de daño Físco a Servidor

Paso	Acción
1	Cuantificar nivel de daño
2	Decidir si la operatividad del equipo se verá comprometida
3	Determinado el daño: remplazar pieza dañada, en caso de contar con garantía contactar al fabricante.
4	Si el daño es grave reestablecer servicios en otro equipo con base al último respaldo

En caso de daño Físco a equipo de Telecomunicaciones

Paso	Acción
1	Remplazar equipo (Switch, router) con equipo similar que se cuente en stock
2	Restaurar la configuración de los respaldos generados.

En caso de daño de enlace de Telecomunicaciones

Paso	Acción
1	Levantar los enlaces redundates, en caso de que se tengan
2	Contactar proveedor de servicios para reparar el daño

Acciones Después la Contingencia

Paso	Acción
1	Validar los servicios publicados por los equipos
2	En caso de remplazo de pieza solicitar la compra de otra para tener el stock
3	En caso de daño de un enlace, una vez reestablecido por parte del proveedor validar la navegación

Contactos para notificación de Emergencias

Nombre	Teléfono Oficina	Celular	Área
Rafael Sánchez Salazar	618 8271281	5554693465	Director de Transformación Digital
Manuel Calderón Perez	618 8271289	6181227895	Soporte Técnico
Gerardo Rodriguez	618 8271289	6182991558	Servidores
Jaime García Navarro	618 8271289	6181706694	Redes
Alvaro Martínez		6182190557	Sistemas

Contacto Proveedores de Servicios

Nombre	Teléfono	Celular	Servicio
Linkware	827 44 10	618 134 42 90	Equipo de red, reparación enlaces
Telmex	01 800 123 12 12		Internet y Telefonía IP
DELL	01 800 727 11 00		Servidores

Electrico		618 181 19 80	Planta de emergencia, conexiones eléctricas
Servicios Generales		618 105 46 79	Infraestructura electrica, mecanica interna

Plan de contingencia Base de Datos

Acciones Preventivas a la Contingencia

Base de Datos

1.- Se realizan respaldos diario de la base de datos (SIIA), dicho respaldo se transfiere a otro equipo fuera del site, como medida preventiva de desastre del site, los respaldos se realizan en discos así como en un servidor de respaldos alterno.

2.- Se respalda el código fuente de los sistemas cada tres meses, cada líder de proyecto realiza el respaldo en disco y es resguardado en la oficina del jefe de sistemas.

Acciones Durante la Contingencia

Base de Datos

1.- Falla en el Servidor o Base de Datos.

a.- El servidor de Prueba se prepara a nivel de discos (Almacenamiento), Sistema Operativo (Actualizaciones) para que tome el rol de producción.

b.- Se toma el último respaldo para su restauración, se contacta a todos los usuarios para que realice una verificación de funcionalidad.

2.- Perdida del Site.

a.- Se ubica un servidor en las áreas estratégicas de telecomunicaciones para su preparación a nivel de discos (Almacenamiento), Sistema Operativo (Actualizaciones) y Software de Base de Datos.

b.- Se toma el último respaldo para su restauración, se contacta a todos los usuarios para que realice una verificación de funcionalidad.

Acciones Después la Contingencia

Base de Datos

Se realiza una evaluación del estado actual de la información por áreas, para determinar el nivel de perdida de información, realizar plan de recuperación de información con las diferentes herramientas de base de datos**.**

Control de Versiones

Fecha	Resumen de Cambios	Realizado por
27/11/2018	Documento Inicial	Coordinación de Telecomunicaciones e informática
04/03/2019	Actualización de información de contactos	Depto. Infraestructura
19/02/2020	Actualización de información de proveedor de Internet y Telefonía	Depto. Infraestructura