CONSEJO REGIONAL
SUR-SURESTE

ANUIES
Al servicio y fortalecimiento de la educación superior

PLAN DE CONTINGENCIAS PARA INSTITUCIONES DE EDUCACIÓN SUPERIOR

Red de seguridad en Cómputo Sur-Sureste

Octubre de 2011

Contenido

I. 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.

Ante tal situación, la red de Seguridad en Cómputo del consejo regional sur-sureste, así como los representantes de Seguridad de la Información de las Instituciones de Educación Superior (IES): Universidad Autónoma de Yucatán (UADY), Universidad Autónoma del Estado de Hidalgo (UAEH), Universidad Autónoma de Aguascalientes (UAA) y Universidad Autónoma de México (UNAM) -Ciencias Nucleares-, hemos coincidido en que los activos de nuestras instituciones representan el elemento fundamental para el préstamo de los servicios educativos y por lo tanto necesitan del desarrollo de lineamientos que favorezcan o propicien su uso racional, así como el desarrollo de procedimientos para garantizar la continuidad del servicio ante cualquier incidente. Esto conlleva a incrementar su efectividad, a mejorar la productividad, eficiencia del personal y a proveer un servicio continuo y eficaz.

El Plan de Contingencias implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por tanto es necesario que el Plan de Contingencias incluya un Plan de Recuperación de desastres, el cual tendrá como objetivo, restaurar el Servicio de Cómputo en forma rápida, suficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo posible. Pese a todas las medidas de seguridad implementadas puede ocurrir un desastre.

Este documento contiene el las recomendaciones generales para la elaboración de un Plan de Contingencia para un IES. El cual podrá servir como un repositorio centralizado para la información, tareas y procedimientos que puedan ser necesarios para facilitar la toma de

decisiones a la administración del IES, así como de desarrollar procesos y definir sus tiempos de respuesta ante cualquier falseo o interrupción extendida de las operaciones normales y servicios de la institución. Esto es especialmente importante si la causa de la interrupción es tal que una pronta restauración de las operaciones no pueda ser realizada empleando solamente procedimientos operacionales de un día normal.

En términos de personal y recursos financieros, las tareas de información y procedimientos detallados en este plan, le demuestran a la administración del IES la importancia de contar con un plan de cómo responder, restaurar y recobrar. Por lo tanto, es esencial que la información y planes de acción de este plan, se mantengan viables y puedan ser mantenidos actualizados para poder asegurar la efectividad en el momento de su ejecución.

2.- Plan de Contingencias

El Plan de Contingencias es el instrumento de gestión para el buen manejo de las *Tecnologías de la Información y las Comunicaciones*. Dicho plan contiene las **medidas técnicas, humanas y organizativas** necesarias para garantizar la continuidad de las operaciones de la institución.

Así mismo, este plan de contingencias sigue el conocido ciclo de vida iterativo "*plan-do-check-act*", es decir, "planifica-actúa-comprueba-corrige". Surge de un análisis de riesgos, donde entre otras amenazas, se identifican aquellas que afectan a la continuidad de la operación de la institución.

El plan de contingencias deberá ser revisado semestralmente. Así mismo, es revisado/evaluado cuando se materializa una amenaza.

El plan de contingencias comprende cuatro planes.

a) Plan de respaldo. Contempla las medidas preventivas antes de que se materialice una amenaza. Su finalidad es evitar dicha materialización.

b) Plan de emergencia. Contempla las medidas necesarias durante la materialización de una amenaza, o inmediatamente después. Su finalidad es contrarrestar los efectos adversos de la misma.

c) Plan de recuperación. Contempla las medidas necesarias después de materializada y controlada la amenaza. Su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

d) Plan en caso de huracanes. Incorpora las acciones, responsables y actividades en caso de una amenaza de huracán.

El plan de contingencias deberá expresar claramente los siguientes aspectos:

1. Qué recursos materiales son necesarios.
2. Quienes están implicados en el cumplimiento del plan, sus responsabilidades concretas y su rol.
3. Acciones a seguir.

Qué recursos materiales son necesarios.

Las instituciones deberán contar con un *Centro de Respaldo Institucional* (CRI), ya sea propietario o arrendatario.

Quienes están implicados en el cumplimiento del plan, sus responsabilidades concretas y su rol.

- Los Administradores de Tecnologías de información (ATI´s) de cada dependencia son los responsables de realizar todas las acciones relacionadas a los planes de contingencia, en cualquiera de sus tres subplanes.

- Los ATI´s deberán realizar todas las actividades establecidas en las políticas del reglamento de seguridad en coordinación con el responsable del CRI y con las áreas involucradas en materia de seguridad institucional.

Acciones a seguir.

- Determinar los requerimientos de los procesos del Centro de Proceso de Datos (CPD), verificando el análisis de riesgos y el análisis de impacto en él.

- Proveer procedimientos de recuperación para restaurar sus datos y servicios de procesamiento.

- Mantener y poner a prueba su solución de recuperación.

3.- Propósito

El propósito de este plan es mantener la continua ejecución de los procesos de misión crítica y sistemas de información tecnológica de la IES 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 IES 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.

4.- Alcance

Proveer información sobre los sistemas, lugares, medidas, limitantes técnicos y limitantes físicas del Plan de Contingencia de la IES.

5.- Objetivos

Proporcionar a la IES 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, así como salvaguardar la integridad física del personal.

Las medidas son, dependiendo de la variedad de sistemas clasificados, de función critica, como son la conectividad, acceso a internet, correo electrónico u otras aplicaciones mayores, como desarrollos propios de sistemas de bases de datos. Por lo tanto muchos de lo eventos y vulnerabilidades pueden ser mitigados aunque algunos de los eventos no puedan ser prevenidos. Es por esto que es importante que el IES desarrolle planes de contingencia y planes de recuperación de desastre para asegurar la ininterrumpida existencia de sus funciones y la continuidad del servicio a sus usuarios y/o clientes.

El principal objetivo de un plan de contingencia gira alrededor de la protección de los dos principales activos de una organización: el personal y la información. Todas las facetas de un plan de contingencia deben orientarse a la protección y salvaguarda del personal, y proteger y recuperar información. El principal objetivo de este plan es establecer las políticas y procedimientos para ser usados para los sistemas de información en el caso de una contingencia, para proteger y asegurar la funcionalidad de estos activos.

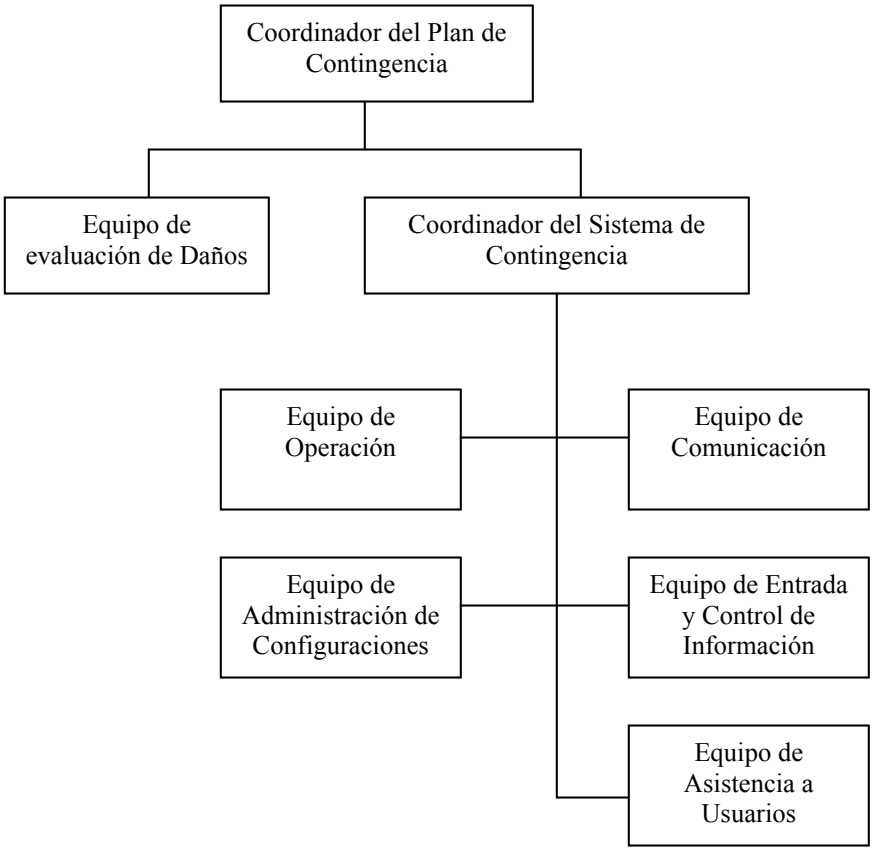
El plan busca los siguientes objetivos:

- Minimizar el número de decisiones que deben ser tomadas durante una contingencia
- Identificar los recursos necesarios para ejecutar las acciones definidas por este plan.
- Identificar las acciones a ser tomadas por equipos pre-diseñados
- 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.

6.- Organización

En el caso de un desastre u otra circunstancia que conlleve la necesidad de operaciones de contingencia, la organización normal de la IES deberá cambiar a una organización de contingencia. La IES deberá centrarse en cambiar, la estructura actual y funciones de un "día normal de trabajo", a la estructura y funciones requeridas por la contingencia trabajando en conjunto para la restauración en tiempo de las operaciones de la misma.

Una estructura propuesta es la que se presenta en el siguiente diagrama:



7.- Fase de Contingencia

El Coordinador del Plan de contingencia del IES, en conjunto con sus directivos, deberá determinar cuales equipos y miembros son responsables de cada función durante las fases:

7.1 Fase de Respuesta

7.2 Fase de Reasunción

7.3 Fase de Recuperación

7.4 Fase de Restauración

8.- Sistemas/aplicaciones/servicios de misión critica

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

Acrónimo del Sistema	Nombre Sistema
Conectividad LAN	*Conexión de Red Interna*
Conectividad WAN	*Conexión de Red Externa*
DNS	Servicio de Resolución de Nombres
Correo	Correo Electrónico Institucional
BD	Base de Datos Institucional

9.- Amenazas

La siguiente tabla muestra las amenazas más comunes que podrían impactar la continuidad y componentes de sistemas y su administración. Las amenazas que son presentadas con (XX) son consideradas las de mayor probabilidad de ocurrir.

Probabilidad de Amenazas			
Probabilidad de Ocurrencia:	**Alta**	**Media**	**Baja**
Falla del aire acondicionado		***X***	
Accidente aéreo			***X***
Chantaje		***X***	
Amenazas de bomba			***X***
Frío / helada / Nieve			***X***
Perdida de comunicación		***X***	
Destrucción de información		***X***	
Terremotos			***X***
Fuego		***XX***	
Inundación / Daño por agua			***X***
Corte eléctrico / Interrupción	***XX***		
Sabotaje / Terrorismo			***X***
Tormentas / Huracanes		***X***	
Vandalismo		***X***	

PLAN DE CONTINGENCIA PARA EL SUMINISTRO DE ENERGÍA ELÉCTRICA EN LA COORDINACIÓN ADMINISTRATIVA DE TECNOLOGÍAS DE INFORMACIÓN.

Acciones Preventivas a la Contingencia

Planta de Emergencia

- Contar con una planta de emergencia que suministre energía regulada en cada site o centro de cableado
- Supervisar semanalmente el nivel óptimo de combustible, agua, baterías, etc.
- Contar con un plan de mantenimiento semestral con supervisiones mensuales
- Supervisar el combustible de respaldo en el área de servicios generales
- Contar con equipo de emergencia contra incendios en el local de la planta
- Contar con el mapa eléctrico del área en la planta y archivado, identificando los contactos respaldados y regulados
- Contar con un procedimiento de operación y uno en caso de un mal funcionamiento
- Contar con tierras físicas independientes a los servicios de telecomunicaciones

By Pass

- Contar con un *By Pass* en cada Site que contenga equipos críticos conectados a la red o al segmento de red (site principal de cada nodo y central)
- Supervisar mensualmente el optimo estado del *By Pass*
- Contar con el mapa eléctrico del área ilustrando el *By Pass*
- Plan de mantenimiento anual integral con supervisiones mensuales
- Contar con un procedimiento de operación y uno en caso de un mal funcionamiento
- Contar con las elementos necesarios para activar y/o desactivar el *By Pass*

UPS

- Contar con un UPS con capacidades necesarias (40% superiores) en todos los Site´s y centros de cableado
- Plan de mantenimiento anual integral con supervisiones mensuales
- Contar con el mapa eléctrico del área, identificando los contactos regulados y respaldados
- Contar con un procedimiento de operación y uno en caso de un mal funcionamiento
- Determinar semestralmente el tiempo efectivo y real de respaldo del UPS con respecto a las diferentes cargas.

Generales

- Contar con un directorio de los responsables del suministro eléctrico en cada nodo
- Contar con un procedimiento para reportar el incidente a las áreas involucradas (Servicios Generales, Telmex, CFE, Proveedores de Mantenimientos, etc.)
- Contar con un procedimiento para notificar a los usuarios afectados la probable baja de los servicios de comunicación
- Contar con procedimiento de ejecución de respaldos de emergencia a la información del servidor Web, mail, DNS, configuraciones de Equipo Activo principales y centrales
- Contar con una tabla de claves de prioridades para dar aviso a los usuarios prioritarios con el fin de optimizar tiempo y recursos
- Solicitar revisión periódica (semestral) del estado y óptimo funcionamiento de los bancos de respaldo eléctrico en los equipos del proveedor de medios.
- Asignar jerarquía a los equipos Activos y Servicios para ejecutar medidas mayores (darlos de baja)
- Determinar las fases de una contingencia de esta índole.

Acciones Durante la Contingencia

En caso de interrupción del suministro eléctrico en lapsos cortos consecutivos

- Comunicarse con servicios generales para la supervisión de la Planta de emergencia
- Monitorear el UPS cada 20 min. para programar acciones mayores
- Valorar la decisión de dar de baja los equipo activos y/o servicios para evitar daños y/o pérdida de información y de equipos

En caso de una interrupción del suministro eléctrico no mayor a una hora

- Comunicarse con servicios generales para la supervisión de la Planta de emergencia
- Monitorear el UPS cada 10 min. para programar acciones mayores
- Apagar los equipos no prioritarios como impresoras, monitores o PC que no demanden su uso
- Desconectar electrodomésticos (cafeteras, equipo de sonido, refrigerador, horno de microondas, ventiladores, etc.)
- Contar con los procedimientos para dar de baja los equipos activos
- Contar con radios de comunicación cargados

En caso de una interrupción del suministro eléctrico mayor a una hora

- Dar aviso de la contingencia a los usuarios prioritarios (Rectoría, Secretaría General, Planeación, Departamento de Sistemas, Centros de Cómputo, Bibliotecas, Centros de Auto aprendizaje, Institutos, Escuelas y Campus).
- Preparar el apagado de los equipos prioritarios (equipo activo)
- Comunicarse con servicios generales para la supervisión de la planta de emergencia con mayor énfasis
- Monitorear el UPS cada 5 min. para programar acciones mayores
- Dar de baja equipo activo y servicios con mediana prioridad con respecto a las fases definidas.

Acciones después de la Contingencia

- Brindar un tiempo de gracia (depende de la magnitud de la contingencia) para restablecer los equipos activos y servicios
- Restablecer los equipos activos y servicios que se dieron de baja, en forma paulatina.
- Validar el correcto funcionamiento de los equipos activos y servicios
- Identificar los posibles daños de los equipos activos
- Notificar a los usuarios afectados el restablecimiento de los servicios y su condición
- Evaluar los daños de los equipos activos, planta de emergencia, UPS y canalizarlos a las áreas involucradas.

PLAN DE CONTINGENCIA PARA LA CONTINUIDAD DE LA OPERACIÓN DEL SERVICIO DE LOS EXPEDIENTES DEL ARCHIVO DE PERSONAL Y CONTROL ESCOLAR

Contenido del plan de contingencias:

1. Lista de números telefónicos de servicios auxiliares y de familiares del personal que labora en el área.
2. Prioridades, responsabilidades y procedimientos para el plan de contingencias.
3. Diagramas de instalaciones.
4. Copias de seguridad.

Acciones preventivas a la contingencia (EXPEDIENTES)

INCENDIOS

Infraestructura

1. La dirección de servicios generales deberá contar con diagramas de instalaciones, el director del área deberá contar con una copia de las mismas.

2. Contar con extinguidores cargados.
3. Capacitación del personal para el uso adecuado de extinguidores por parte de servicios de bomberos.
4. Contar con señalamientos de rutas de evacuación.
5. Contar con lámparas emergentes con batería.
6. Realizar simulacros una vez por año en la dirección.
7. Contar con sistemas de alarmas.

Servidores

1. Contar con respaldos internos y externos.
2. Apagar servidores no prioritarios.

HUMEDAD

Infraestructura

1. Dar mantenimiento preventivo una vez por año con impermeabilizantes a los techos y paredes donde exista el riesgo de humedad.

2. Mantener ventilación en el área de archivo.

3. Fumigar las áreas una vez por año para evitar alergias provocadas por la humedad (moho, insectos)

4. Colocar en lugares seguros el hardware, software y documentos importantes.

5. Apagar equipos de cómputo prioritarios.

Servidores

1. Contar con bolsas de plástico para cubrir servidores y documentos importantes que puedan mojarse.

ROBO O EXTRAVIO

Infraestructura

1. Colocar letreros o anuncios que impidan el acceso al personal no autorizado.
2. Que el personal autorizado cuente con identificación.
3. El lugar físico donde se encuentran resguardados los expedientes sea un lugar aislado y seguro.

Servidores

1. Evitar el acceso a personal no autorizado al área de servidores.(solamente el administrador)

Documentación

1. Contar con vales de salida de expedientes autorizado por el jefe del área.
2. Vigilancia del personal que labora en el área de archivo.

Acciones durante la Contingencia (EXPEDIENTES)

INCENDIOS

Infraestructura

1. El director del área deberá contar con una copia de las instalaciones del área de trabajo.
2. Utilizar los extinguidores por personal capacitado.
3. Respetar los señalamientos de rutas de evacuación.
4. Si es necesario, utilizar lámparas emergentes con batería.
5. Activar el sistema de alarmas.

Servidores

1. Asegurar que se tengan los respaldos externos
2. Apagar servidor.

HUMEDAD

Infraestructura

1. Abrir ventanas para mantener la ventilación en el área de archivo.
2. Colocar en lugares seguros el hardware, software y documentos importantes.
3. Apagar equipos de cómputo prioritarios.

Servidores

1. Cubrir con bolsas de plástico servidores y documentos importantes que puedan mojarse.
2. Colocar los *no-breaks* sobre mesas

ROBO O EXTRAVIO

Personal

1. El personal que labora en el área deberá reportar el extravío o robo al jefe inmediato y en su caso a la dirección general jurídica para su investigación.
2. Tratar de localizar a la persona que extrajo el expediente.

Documentación

1. Buscar el vale de salida de expedientes autorizado por el jefe del área.

Acciones después de la contingencia (EXPEDIENTES)

1. Realizar un reporte de los daños

2. Que el personal encargado del área de contingencia se reúna para analizar el plan de continencias y realizar las modificaciones correspondientes, así como las funciones o acciones del personal de contingencias.

PLAN DE CONTINGENCIA PARA CUIDAR LA INTEGRIDAD DEL PERSONAL

Acciones antes de la contingencia

- Programar 2 simulacros al año
- Programar dos fumigaciones anuales, en periodos vacacionales
- Contar con botas e impermeables para poder entrar y salir de la DBCI
- Conocer el manejo de los extintores
- Contar con batas, guantes y cubre bocas para el manejo del acervo
- Contar con botiquines de primeros auxilios en áreas estratégicas
- Contar con capacitación de primeros auxilios
- Implementar alarmas de emergencia en lugares estratégicos dentro de la DBCI
- Establecer puntos de reunión dentro y fuera de la DBCI
- Difundir las rutas de evacuación, así como los sitios de localización de alarmas, extintores
- Establecer procedimientos de evacuación
- Capacitación permanente y actualizada a los comités de Seguridad e Higiene y al de Seguridad en Cómputo
- Contar con un directorio del personal

Acciones durante la contingencia

- Accionar las alarmas de emergencia
- Utilizar las botas e impermeables para poder salir o ingresar a la DBCI en caso de inundación
- Dirigir a los usuarios en la evacuación e información de salidas de emergencia
- Priorizar la evacuación
- Llamar al 066

Acciones después de la contingencia

- Brindar los primeros auxilios a las personas que lo requieran.
- Realizar un recuento de los daños causados.
- Realizar un informe con los hallazgos y emitir a la Dirección.
- Tomar acciones de acuerdo al informe emitido.
- Retroalimentar los planes de contingencia con lo aprendido en la ultima contingencia.

DOCUMENTOS NECESARIOS PREVIOS A LAS CONTINGENCIAS.

- Contar con una copia del inventario del mobiliario y equipo existente en el área.
- Contar con un listado de configuraciones del equipo de cómputo y telecomunicaciones que reside en el área.
- Contar con documentación al día de contratos de mantenimiento de infraestructura.

10. Ejemplo de contenido del plan de contingencia para una IES.

- Listas de notificación, números de teléfono, mapas y direcciones
- Prioridades, responsabilidades, relaciones y procedimientos
- Información sobre adquisiciones y compras
- Diagramas de las instalaciones
- Sistemas, configuraciones y copias de seguridad en cinta

Acciones preventivas.

En caso de Huracán o tormenta tropical, seguir las siguientes medidas de prevención:

a) Infraestructura

1. Mantener el tanque de gasolina del automóvil lleno. Los vales pueden ser solicitados al Coordinador Administrativo.
Responsable: (la IES debe especificar el nombre del responsable de la actividad).

2. Realizar mantenimiento general de la planta eléctrica de emergencia.
Responsable: (la IES debe especificar el nombre del responsable de la actividad).

3. Mantener tanque de la planta de emergencia lleno de diesel.

Responsable: (la IES debe especificar el nombre del responsable de la actividad).

Tener un tambor de Diesel lleno.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Comprar pilas para lámpara de emergencia.

Responsable: (la IES debe especificar el nombre del responsable de la actividad).

Dar servicio de impermeabilizante a los techos y/o paredes.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Agua. Contar con agua purificada, mínimo tres botellones.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Contar con impermeables.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Encintar ventanas y sellar puerta trasera y delantera de la coordinación donde se pueda filtrar agua.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Tener a la mano el mapa eléctrico del lugar.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

b) Equipos de Telecomunicaciones

Mantenimiento anual de mayo a junio de las torres de comunicaciones. Enlistar por DES instalaciones vulnerables.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Aislar equipos que estén en riesgo, p.e., en el piso.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Dejar en funcionamiento el servicio de acceso remoto a servidores y equipos de Telecomunicaciones.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)
c) Servidores

Sacar relación de servicios prioritarios: DNS, correo electrónico, Real Audio, Web, Conmutada e Internet.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Apagar Servidores no prioritarios
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Tapar con bolsas de plástico servidores que pueden mojarse
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Poner sobre mesas los no-breaks de servidores
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Generar los últimos respaldos
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Poner en un lugar distante los respaldos de información
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

d) Telecomunicaciones

Sacar relación de equipos prioritarios
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Apagar equipos no prioritarios
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Tapar con bolsas de plástico equipos de comunicaciones que pueden mojarse
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Poner sobre mesas los no-breaks de equipos de comunicaciones
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Generar respaldos de configuraciones e imprimirlos
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

e) Servicios de Información

Contar del mes de junio al mes de octubre con una liga permanente hacia Centros de Información de Huracanes.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

En caso de amenaza de Huracán, dejar liga sobre el estado del fenómeno e información de servicio a la comunidad: albergues, teléfonos de emergencia, etc.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Enviar comunicado a los Directivos y ATI's sobre plan de contigencia y emergencia, indicando números disponibles para reportes y soporte.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Coordinador Administrativo y Responsables de área contar con computadora portatil con carga en pila para estar pendientes de los servicios de TI de la IES en caso de emergencia.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Tener disponibles los números telefónicos del personal de la Coordinación Administrativa y de los responsables de redes de las dependencias universitarias.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Contar una línea telefónica analógica con dispositivo analógico.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Tener los teléfonos celulares con carga completa.
Responsables: Todos

Imprimir hojas de reporte para llevar control de reportes por escrito.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Durante la Contingencia

a) Infraestructura
b)

1. Si la planta se encuentra en funcionamiento no se deberán conectar equipos con motor como refrigerador y no se proporcionará el servicio de carga de teléfonos celulares.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

2. Contar con mangueras y embudo para poner diesel, llevando extinguidor por si se requiere.
Responsable: Se irán turnando: (la IES debe especificar los nombres de responsables de la actividad)

3. En caso de que la planta haya trabajado más de 72 horas sin parar, se recomienda hablar a proveedor para mantenimiento.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

b) Telecomunicaciones

Verificación de enlaces hacia Internet Conmutadas y servidores, paulatinamente verificación de enlaces a DES, generando relación de los que ya están en funcionamiento.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Verificación de estado de los equipos y secado de los mismos en caso necesario
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Levantamiento de reportes de DES con problemas y establecimiento de prioridades para atención.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

c) Servidores

Verificación de servicios de TI prioritarios de la IES.
Responsable: (la IES debe especificar el nombre del responsable de la actividad)
Verificación de estado de los equipos y secado de los mismos en caso necesario

Responsable: (la IES debe especificar el nombre del responsable de la actividad)
Levantamiento todos los servicios adicionales
Responsable: (la IES debe especificar el nombre del responsable de la actividad)

Ejemplo de comunicado a enviar a usuarios de los servicios de TI

Estimados Directores y Administradores de Tecnologías de Información de la IES.

Como parte del proceso para "Proveer los servicios de Tecnologías de Información" de nuestro Sistema de Gestión de Calidad Institucional y ante la temporada de Huracanes del presente año que inicia el 1ro. de junio del presente, es recomendable adoptar un Plan de Contingencia, que permita en lo posible dejar en buen resguardo la infraestructura de nuestra Institución, minimizando los efectos que se pudiesen presentar. Anexo al presente encontrarán el Plan correspondiente (esta información también está publicada en el portal de internet de la IES)

Otro sitio que puede ser de su interés, es la sección del estado del tiempo, al cual pueden acceder desde el portal institucional de la IES en Internet:

http://www.IES.mx/clima.html

en este sitio encontrarán información actualizada de los niveles de alerta de nuestro estado emitido por el Gobierno del Estado de Yucatán, así como una liga al Centro de Huracanes de Miami (NOAA).
Esperando que esta información les sea de utilidad, quedo de Uds.
Atentamente

Centro de operaciones de la Red de la IES

11. Ejemplo de plan de contingencia para una ies en temporada de huracanes

Acciones preventivas.

1.- Equipos de Comunicaciones y Servidores:

a) Sacar respaldos de información de la Dependencia de Educación Superior (DES).
b) Apagar y desconectar equipos de cómputo y comunicaciones, incluyendo no-breaks.
c) Colocar los equipos, incluyendo los no-breaks sobre mesas.
d) Alejar los equipos de las ventanas o de alguna posible entrada de viento o agua.
e) Verificar el funcionamiento de servicios de respaldo, tales como: infinitum de DES, Citrix, VPNs, en su caso.

2.- Infraestructura física y servicios:

a) Contar con impermeables, lámparas de emergencia, jergas, cinta.
b) Encintar ventanas.
c) Cubrir los equipos con bolsas de plástico

3.- Sistema de comunicación con personal:

a) Contar con línea telefónica analógica y teléfono analógico que no requiera alimentación eléctrica.
b) Mantener los teléfonos celulares cargados.
c) Tener impreso los directorios del personal de emergencia (proveedores y personal de CATI)

4.- DES que cuentan con Planta de Emergencia:

a) Realizar mantenimiento general de la planta eléctrica de emergencia.
b) Mantener tanque lleno de diesel.
c) Tener un tambo de diesel lleno.

5. Vehículos
a) Llenar los vehículos con combustible.

Después de la tormenta tropical/huracán

1. Revisión de daños en las ventanas del centro de comunicaciones, centro de cómputo y/o áreas correspondientes. En su caso aislar los equipos afectados o en amenaza. Limpiar y secar pisos.

2. Verificar el funcionamiento de las líneas telefónicas.

3. Secar los equipos no breaks antes de encenderlos a fin de evitar que exploten por exceso de humedad; en lo posible con compresor de aire.

4. Secar los equipos de comunicaciones y posteriormente verificar que los equipos estén en funcionamiento.

5. En caso de contar con enlace inalámbrico, verificar posibles daños en la infraestructura de torre de comunicaciones.

6. Proporcionar las facilidades de acceso a los centros de comunicaciones al personal de la Coordinación Administrativa de Tecnologías de Información, para la realización de configuraciones de respaldo en caso de requerirse.

Ponemos a su disposición los números telefónicos de la Coordinación Administrativa de Tecnologías de Información.

Teléfono: XXXXXXX

Celulares:
La IES deberá indicar el directorio telefónico

12. Ejemplo de políticas de continuidad y contingencia de los servicios

Artículo 12. Respaldos
1.- La información crítica de las Dependencias (correo electrónico, información administrativa y académica) será respaldada diariamente en forma automática y manual, según los procedimientos generados para tal efecto.

2 Los respaldos de la información crítica deberán ser almacenados en un lugar seguro y distante del sitio de trabajo.

3. La DES contará con un plan de contingencia para dar continuidad a los servicios de información definidos como críticos.

Plan de Contingencia en Caso de Tormenta Tropical o Huracan

Acciones Preventivas

1) Equipos de Comunicaciones y Servidores

a. Apagar y desconectar equipos de cómputo y comunicaciones, incluyendo no-breaks.

b. Colocar los equipos, incluyendo los no-breaks sobre mesas.

c. Alejar los equipos de las ventanas o de alguna posible entrada de humedad.

2) Infraestructura física y servicios

a. Contar con impermeables.

b. Encintar ventanas.

c. Cubrir lo equipos con bolsas de plástico

d. Sacar los respaldos de información de la DES.

3) Sistema de comunicación con personal.-

a. Contar una línea telefónica analógica con dispositivo analógico, en su caso conectar un teléfono analógico en la línea ISDN de su DES.

b. Tener los teléfonos celulares cargados.

Acciones después de la Tormenta Tropical/Huracán

4) Revisión de daños en las ventanas del centro de comunicaciones, centro de cómputo y/o áreas correspondientes; en su caso aislar los equipos afectados o en amenaza.

5) Verificar el funcionamiento de las líneas telefónicas.

6) Secar los equipos no breaks antes de encenderlos a fin de evitar que exploten por exceso de humedad.

7) Secar los equipos de comunicaciones y posteriormente verificar que los equipos esten en funcionamiento.

8) En caso de contar con enlace inalámbrico, verificar posibles daños en la infraestructura de torre de comunicaciones.

9) Proporcionar las facilidades de acceso a los centros de comunicaciones, al personal de la Coordinación Administrativa de Tecnologías de Información para la realización de configuraciones de respaldo en caso de requerirse.

REQUISITOS

Redundancia servicios	1. Utilización de los servicios de la nube. 2. Utilización de redes privadas virtuales (VPNs). 3. Disponibilidad de equipos de comunicaciones obsoletos.
Protección eléctrica	Mantenimiento semestral de la planta: limpieza y verificación de los niveles y en caso su completar diesel, aceite, refrigerante y líquidos para acumuladores.
Redundancia comunicaciones	1. Equipos de respaldo: switches, ruteadores, bridges, módulos de equipos de comunicaciones.
Enlaces	1. Enlace inalámbrico 2. Enlaces digitales. 3. Equipo con módem y línea telefónica analógica. 4. Enlaces alternativos a ISP
Personal	Guardia permanente

REFERENCIAS BIBLIOGRÁFICAS.

Cano Jeimy J. (2004). Inseguridad informática. Un concepto dual en seguridad informática. Consultado en Marzo 12, 2010. Consultado en: http://www.acis.org.co/index.php?id=83

Mark Wilson, Joan Hash,(2003) Building an Information Technology Security Awareness and Training Program, NIST Special Publication 800-50, National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

McCarthy Linda (2003). IT Security-Risking the Corporation. Prentice Hall

National Institute of standards an Technology. Consultado el 20 de septiembre de 2010 en el URL:
http://www.google.com.mx/url?sa=t&rct=j&q=contingency%20plan%20template&source=web&cd=1&sqi=2&ved=0CCEQFjAA&url=http%3A%2F%2Fcsrc.nist.gov%2Fgroups%2FSMA%2Ffasp%2Fdocuments%2Fcontingency_planning%2Fcontingencyplan-template.doc&ei=uaUUT-_0JYGFsALW2tCEBA&usg=AFQjCNFVijqbe1NJ2ldgdUN_AVVJGhKc4Q&sig2=scEVVZHHLIWaThThGr52Mg&cad=rja

Patriick D. Howard, 2003, "The Security Policy Life Cycle: Functions and REsponsibilities", Tipton & Krause CRC Press LLC, 2003.

Swason M., Bartol N., Sbato J., Joan H.,& Graffo L., (2003) Security Metrics Guide for Information Technology Systems. Consultado el febrero 5, 2010 del sitio de National Institute of Standards Administration U.S. Department of Commerce http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf

Whitman Michael, Mattord Herbert. (2004). Management of information security. Boston, Massachusetts: Thomson Course Technology.