## Propósito

El Plan de Recuperación de Desastres está diseñado para asegurar la continuidad de los procesos críticos del Centro de Datos del área de tecnologías de la información del INSTITUTO ESTATAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES ante cualquier evento catastrófico que pueda presentarse. Este plan proveerá de un conjunto de soluciones efectivas y/o recomendaciones que podrán ser utilizadas para reducir el impacto del desastre en la operación del instituto.

## Alcance

Se considerarán eventos críticos tales como una interrupción prolongada de la electricidad, huracanes, inundaciones, incendios, vandalismo y sismos/terremotos, los cuales serán abordados a detalle en los siguientes apartados.

## Procedimientos de Emergencia

En una situación de desastre lo más importante es evacuar de forma segura a todo el personal del área de tecnologías de la información para evitar daños que atenten contra la vida de éstos, ninguno de los procedimientos enlistados en este presente plan deberán tener prioridad sobre los procedimientos de evacuación emitidos por el instituto; los procedimientos de evacuación institucional deberán ser seguidos de forma inmediata.

Después del acontecimiento y cuando las autoridades lo consideren seguro el área de tecnologías de la información evaluará el impacto sobre las instalaciones y el equipamiento para tomar las decisiones que correspondan para llevar a cabo la recuperación.

## Fallas en la Red de Distribución Eléctrica

Se considera una falla en la red de distribución eléctrica una interrupción prolongada de la alimentación eléctrica si tiene una duración de más de 24 horas o bien cuando exista una variación alta en el suministro eléctrico que podría afectar de manera permanente la operación del centro de datos.

Para dar solución a esta situación, puede considerarse lo siguiente:

|  |  |
| --- | --- |
| **Antes** | * Verificar que los sistemas de respaldo de la información institucional se encuentren funcionando en óptimas condiciones.
* Verificar que el inventario de sistemas, equipo de red y cómputo se encuentre lo más actualizado posible.
* Verificar que el plan de contingencia informático se encuentre actualizado.
* Realizar revisiones periódicas de la red eléctrica del centro de datos.
* Revisar periódicamente el estado de las baterías de los sistemas de respaldo (UPS) para aquellos dispositivos electrónicos sensibles en el centro de datos.
* Sustituir equipos obsoletos y desconectar equipos en desuso.
* Emitir lineamientos y/o recomendaciones para garantizar el funcionamiento óptimo de la red eléctrica del centro de datos.
 |
| **Durante** | * Desconectar todos los equipos en el centro de datos para evitar daños por variaciones altas de voltaje cuando regrese el suministro eléctrico.
* Notificar a los jefes de departamento del instituto sobre los servicios afectados y posibles tiempos de respuesta.
* Reportar falla en el servicio al suministrador de energía eléctrica del centro de datos.
* En caso de que la falla esté de nuestro lado contactar a un técnico especializado para que realice los diagnósticos y reparaciones pertinentes.
* Habilitar espacios de trabajo temporales para llevar a cabo las funciones esenciales.
* Considerar un sitio alterno donde puedan ser instalados los equipos indispensables para llevar a cabo las actividades fundamentales para la operación del centro de datos.
* Suplir energía eléctrica mediante sistemas de emergencia.
 |
| **Después** | * Revisar el estado de los equipos de red y cómputo tras falla en el suministro eléctrico.
* Reconectar los equipos de red y cómputo que se encuentren en buen estado tras falla del suministro eléctrico.
* Sustituir los equipos afectados por las fallas de la energía eléctrica.
* Notificar a los jefes de departamento del instituto sobre los servicios afectados y posibles tiempos de respuesta.
* Diagnosticar probables causas de la falla y de ser posible emitir una recomendación para evitar que vuelva a suceder la falla.
 |

## Huracanes

Los huracanes son un fenómeno meteorológico peligroso y destructivo con vientos de alta intensidad, tormentas eléctricas, lluvias cuantiosas y constantes, usualmente se puede predecir su llegada con 48 a 72 horas de anticipación.

Considerando que el estado de Yucatán es una zona frecuentemente impactada por huracanes se consideró separar este fenómeno meteorológico del apartado con las inundaciones para darle tareas específicas a realizar.

Para dar solución a esta situación, puede considerarse lo siguiente:

|  |  |
| --- | --- |
| **Antes** | * Verificar que los sistemas de respaldo de la información institucional se encuentren funcionando en óptimas condiciones.
* Verificar que el inventario de sistemas, equipo de red y cómputo se encuentre lo más actualizado posible.
* Verificar que el plan de contingencia informático se encuentre actualizado.
* Estar al pendiente de los mensajes que las autoridades en materia de protección civil emitan sobre el estado actual del huracán.
* Apagar y desconectar toda la infraestructura del centro de datos 24 a 12 horas antes de la llegada del huracán.
* Resguardar aquellos equipos que pudieran estar expuestos a daños severos por las ráfagas de viento al estar expuestos al exterior como son antenas de interconexión inalámbrica, puntos de acceso, cámaras de vigilancia y sensores inalámbricos.
* Notificar a los jefes de departamento del instituto sobre los servicios afectados y posibles tiempos de respuesta.
* En caso de que alguna infraestructura fuera fundamental para la operación del instituto (aun durante la emergencia) mover la infraestructura de manera temporal a un sitio alterno.
 |
| **Durante** | * Estar al pendiente de los mensajes que las autoridades en materia de protección civil emitan sobre el estado actual del huracán y zonas de afectación.
* En la medida de lo posible monitorear el estado de la infraestructura fundamental para ver si hay alguna afectación en los servicios.
 |
| **Después** | * Limpiar áreas afectadas del centro de datos por el paso del huracán.
* Revisar el estado de los equipos de red y cómputo tras el paso del huracán.
* Reconectar todos los equipos de red y cómputo en buen estado que fueron apagados durante el paso del huracán.
* Reinstalar todos los equipos fueron resguardados como medida preventiva antes de la llegada del huracán.
* Sustituir los equipos afectados por el huracán.
* Notificar a los jefes de departamento del instituto sobre los servicios afectados y posibles tiempos de respuesta.
 |

## Inundaciones

Se considera el caso en que se presente una inundación, resultado de lluvias prolongadas o

abundantes a causa de un fenómeno meteorológico, o algún desperfecto en la tubería hidráulica y que por consecuencia pueda afectar las instalaciones del centro de datos, que a su vez ponga en riesgo la integridad física de la información, los equipos de cómputo, servidores y mobiliario.

Para dar solución a esta situación, puede considerarse lo siguiente:

|  |  |
| --- | --- |
| **Antes** | * Verificar que los sistemas de respaldo de la información institucional se encuentren funcionando en óptimas condiciones.
* Verificar que el inventario de sistemas, equipo de red y cómputo se encuentre lo más actualizado posible.
* Verificar que el plan de contingencia informático se encuentre actualizado.
* Verificar que se le esté dando mantenimiento preventivo a los drenajes y sistemas de alcantarillados cercanos al centro de datos.
* Verificar que la infraestructura de red y cómputo sensible no se encuentre en el piso donde pudieran verse más afectados durante una inundación.
* Verificar que los equipos de respaldo como UPS o reguladores de voltaje del centro de datos se encuentren aterrizados para evitar que un cortocircuito ocasione daños graves a la infraestructura de red y de cómputo durante el paso de una inundación.
 |
| **Durante** | * Desconectar el suministro de energía eléctrica al centro de datos para evitar posibles daños ocasionados por la inundación.
* Notificar a los jefes de departamento del instituto sobre los servicios afectados y posibles tiempos de respuesta.
* Resguardar los equipos de red y de cómputo que están siendo dañados por las inundaciones en una zona seca y fuera de peligro.
* Aquellos equipos que no puedan ser movidos por que están empotrados (racks, escaleras, reguladores de voltaje, etc.) en la medida de lo posible deberán ser cubiertos con materiales que eviten que el agua los siga dañando.
 |
| **Después** | * Limpiar áreas afectadas del centro de datos por la inundación.
* Revisar el estado de los equipos de red y cómputo afectados por la inundación.
* Reinstalar todos los equipos fueron resguardados durante la inundación.
* Restaurar el suministro de energía eléctrica al centro de datos.
* Sustituir los equipos afectados por la inundación.
* Notificar a los jefes de departamento del instituto sobre los servicios afectados y posibles tiempos de respuesta.
* Notificar a las autoridades pertinentes sobre los sistemas de alcantarillado público en mal estado.
 |

## Incendios

Los incendios son considerados como situaciones de emergencia con una ocurrencia más frecuente en el ambiente laboral, su magnitud puede ser desde un simple contacto eléctrico en mal estado, fácilmente controlable, hasta un incendio de grandes proporciones.

El presente plan sólo contempla las acciones a realizar para aquellos fuegos que sean

considerados como de riesgo menor y que puedan ser controlados con extintores de incendio

portátiles u otros medios y que no representen un peligro para la integridad física del personal del área de tecnologías de la información.

Los incendios mayores a los descritos con anterioridad serán controlados por las autoridades correspondientes como el cuerpo de bomberos del municipio.

Para dar solución a esta situación, puede considerarse lo siguiente:

|  |  |
| --- | --- |
| **Antes** | * Verificar que los sistemas de respaldo de la información institucional se encuentren funcionando en óptimas condiciones.
* Verificar que el inventario de sistemas, equipo de red y cómputo se encuentre lo más actualizado posible.
* Verificar que el plan de contingencia informático se encuentre actualizado.
* Verificar que los extinguidores se les esté dando el mantenimiento periódicamente.
* Tener disponible al menos un extinguidor con un agente no conductor de electricidad para apagar los incendios en el centro de datos.
* Capacitar al personal sobre qué hacer en caso de incendio y sobre el uso de los extinguidores adecuados para los diferentes tipos de incendios.
* Verificar que las líneas eléctricas del centro de datos no se encuentren sobrecargadas y sigan los estándares nacionales para evitar incendios en las instalaciones eléctricas.
* No permitir productos inflamables dentro y cerca del centro de datos.
* No permitir fumar dentro y cerca del centro de datos.
* Verificar el funcionamiento de los sistemas de detección de incendios y de gases inflamables cerca del centro de datos.
 |
| **Durante** | * Si el incendio tiene poca magnitud intentar apagarlo con un extinguidor.
* Desalojar el centro de datos utilizando las rutas de evacuación establecidas, cubriendo boca y nariz con tela húmeda, si el humo es excesivo, desplazarse rápidamente para evitar la intoxicación por inhalación de humo.
* Cortar el suministro de energía eléctrica al centro de datos.
* Notificar lo más pronto posible al cuerpo de bomberos y autoridades correspondientes sobre el posible origen y causa del incendio.
 |
| **Después** | * Limpiar áreas afectadas del centro de datos por el incendio.
* Revisar el estado del equipo de red y de cómputo dañado por el incendio en el centro de datos.
* Revisar el estado de la infraestructura de distribución eléctrica del centro de datos.
* Sustituir los equipos afectados por el incendio.
* Notificar a los jefes de departamento del instituto sobre los servicios afectados y posibles tiempos de respuesta.
* Diagnosticar probables causas del incendio y de ser posible emitir una recomendación para evitar que otro incendio vuelva a dañar la infraestructura en el centro de datos.
 |

## Actos de Vandalismo

Se considera un acto de vandalismo a aquellas catástrofes que fueron causadas deliberadamente por personal del instituto o ajenos a este.

Este supuesto contempla como actos de vandalismo a los ataques cibernéticos, robos, huelgas, manifestaciones con violencia, daños intencionales al equipo de red y/o cómputo o cualquier otro tipo de actividad criminal que perjudique la operación del centro de datos del área de tecnologías de la información.

Para dar solución a esta situación, puede considerarse lo siguiente:

|  |  |
| --- | --- |
| **Antes** | * Verificar que los sistemas de respaldo de la información institucional se encuentren funcionando en óptimas condiciones.
* Verificar que el inventario de sistemas, equipo de red y cómputo se encuentre lo más actualizado posible.
* Verificar que el plan de contingencia informático se encuentre actualizado.
* Establecer un plan de acción de qué hacer en caso de que la información robada o siniestrada pudiera ser considerada como confidencial o reservada (documento de seguridad).
* Capacitar al personal del instituto sobre cómo resguardar su información y sus equipos de cómputo ante una situación de vandalismo.
* Reforzar la seguridad física del centro de datos para retrasar o impedir por completo el acceso no autorizado al centro de datos.
* Reforzar las medidas de seguridad y control de acceso a los servidores y sistemas de acuerdo a estándares internacionales de seguridad de la información.
 |
| **Durante** | * En caso de robo o manifestaciones con violencia notificar a las autoridades correspondientes sobre lo sucedido.
* En caso de un ataque cibernético se aíslan los servidores o sistemas afectados para su análisis forense y se reportan los hechos a las autoridades correspondientes.
* En caso de que el daño haya sido ocasionado por personal del instituto, notificar al departamento de administración y finanzas lo acontecido para deslindar responsabilidades.
* En caso de huelga se debe considerar establecer un sitio alterno para llevar a cabo las operaciones fundamentales del instituto, mientras se recupera el acceso al centro de datos.
 |
| **Después** | * Sustituir los equipos que fueron dañados o robados.
* Notificar a los jefes de departamento del instituto sobre los servicios afectados y posibles tiempos de respuesta.
* Elaborar un reporte con las razones y medidas de seguridad que fallaron, emitiendo acciones a realizar para que no vuelva a suceder el acto de vandalismo.
 |

##

## Sismos

Los sismos son movimientos de la corteza terrestre de corta duración e intensidad variable y son producidos a consecuencia de la liberación repentina de energía, los sismos ocurren sin previo aviso y tienen como peligro principal el derrumbamiento de edificios, incendios y roturas de líneas de gas, entre otros daños graves.

La actividad sísmica en la península de Yucatán es poco numerosa y de muy baja magnitud, por lo que es un evento catastrófico muy poco probable.

Para dar solución a esta situación, puede considerarse lo siguiente:

|  |  |
| --- | --- |
| **Antes** | * Verificar que los sistemas de respaldo de la información institucional se encuentren funcionando en óptimas condiciones.
* Verificar que el inventario de sistemas, equipo de red y cómputo se encuentre lo más actualizado posible.
* Verificar que el plan de contingencia informático se encuentre actualizado.
* Verificar que el equipo de cómputo y equipo de red se encuentren perfectamente asegurados al rack.
* Verificar que el rack, mobiliario y equipos de emergencia se encuentren asegurados al piso.
 |
| **Durante** | * Seguir procedimientos de evacuación institucional.
 |
| **Después** | * Notificar a los jefes de departamento del instituto sobre los servicios afectados y posibles tiempos de respuesta.
* Revisar el estado del equipo de red y de cómputo dañado por el sismo en el centro de datos.
* Revisar el estado de la infraestructura de distribución eléctrica del centro de datos.
* Sustituir los equipos afectados por el sismo.
* Establecer un sitio alterno para llevar a cabo las operaciones fundamentales del instituto, mientras se recupera el acceso al centro de datos.
 |

## Desastre Total

Un desastre total se refiere cuando queda inoperante la mayor parte de los recursos con los que cuenta el centro de datos del área de tecnologías de la información, para desempeñar sus actividades.

Para reducir el impacto de este evento en el centro de datos, es recomendable realizar las siguientes actividades:

|  |
| --- |
| 1. Ubicar un sitio alterno para reanudar las operaciones fundamentales del instituto.
2. Restaurar los sistemas necesarios para la operación fundamental del instituto dando prioridad a los sistemas de manejo de incidentes.
3. Implementar una VPN para el uso de aquellos usuarios que no puedan trasladarse al nuevo sitio de operaciones.
4. Elaborar respaldos de los datos generados en las nuevas instalaciones de forma diaria.
5. Elaborar reporte de daños.
6. Elaborar lista de materiales que se requerirán para reanudar las operaciones del centro de datos del área de tecnologías de la información.
7. Elaborar un reporte donde se evalúe la efectividad de las medidas preventivas presentes en este plan frente a la catástrofe total.
 |

## Directorio

A continuación, se listan al personal del área de tecnologías de la información a cargo de activar y coordinar las actividades de respuesta y recuperación de un incidente no planeado.

|  |
| --- |
| **Nombre**: I.S.C. Juan José May Uc M.T.I.**Cargo**: Coordinador de Sistemas**Correo Electrónico**: juanmay@inaipyucatan.org.mx**Teléfono**: 9999258631 ext. 800 |
| **Nombre**: I.S.C. Leidy Vanesa Magaña Zaldívar**Cargo**: Auxiliar en Administración y Soporte Técnico**Correo Electrónico**: vanesamagana@inaipyucatan.org.mx**Teléfono**: 9999258631 ext. 801 |
| **Nombre**: Jorge Iván Burgos Aguilar**Cargo**: Auxiliar de Redes y Seguridad Informática**Correo Electrónico**: jorgeburgos@inaipyucatan.org.mx**Teléfono**: 9999258631 ext. 802 |

##