

"2019. Año del Centésimo Aniversario Luctuoso de Emiliano Zapata Salazar. El caudillo del Sur".

INTRODUCCIÓN

El plan de contingencia del TESCH ante la posible pérdida, destrucción, robo y otras amenazas, es abarcar la preparación e implementación de un completo plan de contingencia Informático.

Cualquier Sistema de Redes de Computadoras (ordenadores, periféricos y accesorios) están expuestos a riesgo y puede ser fuente de problemas. El Hardware, el Software están expuestos a diversos Factores de Riesgo Humano y Físicos. Estos problemas menores y mayores sirven para retroalimentar nuestros procedimientos y planes de seguridad en la información. Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (el disco duro), bien por grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informático, etc.) que producen daño físico irreparable.

Para realizar el Plan de contingencia informático en el Tecnológico de Estudios Superiores Chicoloapan se tiene en cuenta la información como uno de los activos más importantes de la Institución, además que la infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función del Tecnológico. Este Plan implica realizar un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y sistemas de información, de forma que se puedan aplicar medidas de seguridad oportunas y así afrontar contingencias y desastres de diverso tipo.



SECRETARÍA DE EDUCACIÓN

SUBSECRETARÍA DE EDUCACIÓN SUPERIOR Y NORMAL

DIRECCIÓN GENERAL DE EDUCACIÓN SUPERIOR

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE CHICULOAPAN

Camino al Monte s/n, col. Loma de Guadalupe, c.p. 56380, Chicoloapan de Juárez, Estado de México.

Tel.: (0155) 6315 6655.

"2019. Año del Centésimo Aniversario Luctuoso de Emiliano Zapata Salazar. El caudillo del Sur".

Objetivo General

Formular un adecuado Plan de Contingencias, que permita la continuidad en los procedimientos informáticos del Tecnológico de Estudios Superiores de Chicoloapan, así como enfrentarnos a fallas y eventos inesperados; con el propósito de asegurar y restaurar los equipos e información con las menores pérdidas posibles en forma rápida, eficiente y oportuna; buscando la mejora de la calidad en los servicios que brinda el TESCH.

Objetivos Específicos

Evaluar, analizar y prevenir los riesgos informáticos que pueda ser suspendida completa o parcialmente la prestación del servicio.

Definiciones:

AMENAZA: probabilidad de ocurrencia, durante un período específico y dentro de un área determinada, de un fenómeno que puede potencialmente causar daños en los elementos en riesgo.

CONTIGENCIA: Evento o suceso que ocurre, en la mayoría de los casos, en forma inesperada y que causa alteraciones en los patrones normales de funcionamiento de una organización.

RIESGO: Se refiere a la cuantificación de los posibles daños ocasionados a los elementos en riesgo como consecuencia de un fenómeno natural o artificial en términos de vidas perdidas, personas heridas, daños materiales y ambientales e interrupciones de la actividad económica.

GRAVEDAD: Se refiere a la magnitud resultante de los daños provocados por un siniestro. Esta es subdividida en ninguna, insignificante, marginal, crítica y catastrófica y se definen según el factor de evaluación (víctimas, pérdidas económicas, suspensión de operación, daño ambiental).

SEGURIDAD: Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

DATOS: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

INCIDENTE: Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

PLAN DE CONTIGENCIA: Es una estrategia que se compone de una serie de procedimientos que facilitan una solución alternativa que permite restituir rápidamente el funcionamiento de los servicios críticos de la Fundación ante la eventualidad que lo afecte de forma parcial o total.



SECRETARÍA DE EDUCACIÓN

SUBSECRETARÍA DE EDUCACIÓN SUPERIOR Y NORMAL

DIRECCIÓN GENERAL DE EDUCACIÓN SUPERIOR

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE CHICOLOAPAN

Camino al Monte s/n, col. Loma de Guadalupe, c.p. 56380, Chicoloapan de Juárez, Estado de México.

Tel.: (0155) 6315 6655.

"2019. Año del Centésimo Aniversario Luctuoso de Emiliano Zapata Salazar. El caudillo del Sur".

ANÁLISIS DE LA EVALUACIÓN DE RIESGOS Y ESTRATEGIAS

Factores de afectan la seguridad física y la infraestructura

Dentro de estos factores se encuentran los riesgos de origen natural como los desastres y los riesgos artificiales como los ataques terroristas. Ambos riesgos tienen su origen de causas externas al Tecnológico y su grado de previsión es muy mínimo. La probabilidad de origen natural es baja, mientras, que los riesgos artificiales son de probabilidad media. De igual forma se encuentran las descargas o cortes eléctricos, los cuales pueden generar interrupción en las labores administrativas que pueden afectar la atención a los usuarios.

Riesgo: Es la vulnerabilidad de un activo o un bien, ante un posible o potencial perjuicio o daño.

Existen distintos tipos de riesgos:

- Riesgos Naturales (Mal tiempo, terremoto, inundaciones, etc.)
- Riesgos tecnológicos (Incendios eléctricos, fallas de energía y accidentes de transmisión y transporte).
- Riesgos sociales (Actos terroristas, desordenes, entre otros).

Tipos de contingencias de acuerdo con el grado de afectación:

- En el mobiliario
- En el equipo computo en general (Procesadores, unidades de disco, impresoras)
- En comunicaciones (ruteadores, nodos, líneas telefónicas)

Posibles daños:

- Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas.
- Imposibilidad de acceso a los recursos informáticos, sean estos por cambios voluntarios o involuntarios, tales como cambio de claves de acceso, eliminación de los archivos o proceso de información no deseado.
- Divulgación de información a instancias fuera de la institución fuera de la institución sea mediante robo.



SECRETARÍA DE EDUCACIÓN

SUBSECRETARÍA DE EDUCACIÓN SUPERIOR Y NORMAL

DIRECCIÓN GENERAL DE EDUCACIÓN SUPERIOR

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE CHICOLOAPAN

Camino al Monte s/n, col. Loma de Guadalupe, c.p. 56380, Chicoloapan de Juárez, Estado de México.

Tel.: (0155) 6315 6655.

"2019. Año del Centésimo Aniversario Luctuoso de Emiliano Zapata Salazar. El caudillo del Sur".

Fuentes de daño:

- Acceso no autorizado.
- Ruptura de las claves de acceso a los sistemas computacionales.
- Desastres naturales (terremotos, inundaciones, falla en los equipos de soportes causados por el ambiente, la red de energía eléctrica o el mal acondicionamiento de los equipos.
- Fallas del personal clave (enfermedad, accidente, renuncias, abandono del puesto de trabajo.)
- Fallas de hardware (fallas en los servidores o falla en el cableado de red, Router, etc.)

Clases de riesgo

- Incendio
- Robo común de equipos y archivos
- Falla en los equipos
- Acción de virus informático
- Fenómenos naturales
- Accesos no autorizados
- Ausencia del personal de sistemas.

Factores asociados con la seguridad lógica

Estos riesgos están asociados con fallas en el funcionamiento de los equipos o de los programas de protección, cuyo deterioro o mal uso pueden generar:

- Daños en Discos duros, controladores de red, etc.
- Fallas en equipos de comunicaciones (switches, Routers)
- Daños graves en los archivos del sistema, por error de Hardware o Software
- Ingreso de virus u otros programas malintencionados que puedan dañar los archivos y los equipos computó.



SECRETARÍA DE EDUCACIÓN
SUBSECRETARÍA DE EDUCACIÓN SUPERIOR Y NORMAL

DIRECCIÓN GENERAL DE EDUCACIÓN SUPERIOR

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE CHICULOAPAN

Camino al Monte s/n, col. Loma de Guadalupe, c.p. 56380, Chicoloapan de Juárez, Estado de México.

Tel.: (0155) 6315 6655.

"2019. Año del Centésimo Aniversario Luctuoso de Emiliano Zapata Salazar. El caudillo del Sur".

ACCIONES CORRECTIVAS

Corresponde al plan de contingencia informático minimizar esta clase de riesgos con medidas preventivas y correctivas sobre cada uno. Es de tener en cuenta que en lo que respeta a fenómenos naturales.

Incendio o fuego

Situación	Acción correctiva
La oficina donde están ubicados los servidores cuenta con un extintor cargado, ubicado muy cerca a esta oficina. De igual forma todos los pisos de la institución cuenta con un extintor debidamente cargados.	Se cumple
Se ejecutó un programa de capacitación sobre el uso de elementos de seguridad y primeros auxilios, a el personal perteneciente a la brigada de emergencia. Lo que es eficaz para enfrentar un incendio y sus efectos.	Se cumple
No se realiza la copia de seguridad diariamente al servidor de Backup.	Realizar copia de seguridad semanalmente al servidor de Backup.

Analizando el riesgo de incendio, es necesario almacenar los Backup en lugares donde la acción calorífica de un incendio no alcance los dispositivos de almacenamiento. Por ende, se colocarán en lugares estratégicamente distantes y cercanos a los extintores, para en caso de emergencia sea más fácil controlar el fuego y proteger los dispositivos de almacenamiento.



SECRETARÍA DE EDUCACIÓN

SUBSECRETARÍA DE EDUCACIÓN SUPERIOR Y NORMAL

DIRECCIÓN GENERAL DE EDUCACIÓN SUPERIOR

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE CHICULOAPAN

Camino al Monte s/n, col. Loma de Guadalupe, c.p. 56380, Chicoloapan de Juárez, Estado de México.

Tel.: (0155) 6315 6655.

"2019. Año del Centésimo Aniversario Luctuoso de Emiliano Zapata Salazar. El caudillo del Sur".

Robo de equipos y archivos

Situación	Acción correctiva
Se toma registro de la hora de entrada y salida de las personas particulares que ingresan a la fundación. En caso de que se presente un incidente, se pasará a mirar las cámaras de seguridad.	Registro de entrada y salida
Hurto a mano armada.	Solicitar la colaboración de la Policía para que realice rondas periódicas por el sector donde se encuentra ubicadas las instalaciones

No se han reportado casos en la cual haya existido manipulación y reubicación de equipos sin el debido conocimiento y autorización del Jefe de Área de Sistemas y el coordinador de Sistemas, esto demuestra que los equipos se encuentran protegidos por cada funcionario autorizado.

Falla en los equipos

Situación	Acción correctiva
La falla en los equipos muchas veces se debe a falta de mantenimiento y limpieza.	Realizar mantenimiento preventivo de equipos por lo menos dos veces al año.
La falla en el hardware de los equipos requiere de remplazo de repuestos de forma inmediata.	Contar con proveedores en caso de requerir remplazo de piezas
El daño de equipos por fallas en la energía eléctrica, requiere contar con dispositivos que amplíen tiempo para apagar correctamente el equipo.	Instalación de Nobreak

Analizando el riesgo de falla de los equipos, es recomendable estar realizando mantenimiento preventivo a los equipos computo e implementar estabilizadores (Nobreak) a los equipos para en caso de una falla de energía eléctrica los dispositivos se puedan apagar correctamente.



SECRETARÍA DE EDUCACIÓN

SUBSECRETARÍA DE EDUCACIÓN SUPERIOR Y NORMAL

DIRECCIÓN GENERAL DE EDUCACIÓN SUPERIOR

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE CHICOLOAPAN

Camino al Monte s/n, col. Loma de Guadalupe, c.p. 56380, Chicoloapan de Juárez, Estado de México.

Tel.: (0155) 6315 6655.

"2019. Año del Centésimo Aniversario Luctuoso de Emiliano Zapata Salazar. El caudillo del Sur".

Acción de virus informático

Situación	Acción correctiva
Se cuenta con un software antivirus para la entidad, pero su actualización no se realiza de forma inmediata a su expiración.	Se busca antivirus con licencia gratuita y que ofescan la mejor proteccion
Únicamente el área de sistemas es la encargada de realizar la instalación de software en cada uno de los equipos de acuerdo con su necesidad.	Se cumple
Los antivirus no se actualizan periódicamente en cada equipo.	Instalar y revisar periódicamente que los antivirus de los equipos sigan con la licencia gratuita, de lo contrario se busca otro antivirus con licencia gratuita. .

Tener actualizado e instalado los antivirus para todos los equipos computo del TESCH para prevenir daños por causa de un virus informático.

Terremoto

- Sin Pérdida O Daños Menores De Las Instalaciones: El siniestro puede afectar únicamente parte de la estructura de las instalaciones, en cuyo caso no se verían afectados los datos, sin embargo, podría ser necesario evacuar las instalaciones trasladando al personal fuera de las instalaciones, el impacto provocaría que las actividades se interrumpirían por unas horas o hasta por un día completo.
- Con Pérdida De Las Instalaciones: La pérdida de las instalaciones afectaría gravemente a las operaciones y los datos pueden verse dañados seriamente. En esta parte de la contingencia es donde se requiere que todas las medidas de emergencia y de recuperación que funcionen adecuada y oportunamente.



SECRETARÍA DE EDUCACIÓN

SUBSECRETARÍA DE EDUCACIÓN SUPERIOR Y NORMAL

DIRECCIÓN GENERAL DE EDUCACIÓN SUPERIOR

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE CHICOLOAPAN

Camino al Monte s/n, col. Loma de Guadalupe, c.p. 56380, Chicoloapan de Juárez, Estado de México.

Tel.: (0155) 6315 6655.

"2019. Año del Centésimo Aniversario Luctuoso de Emiliano Zapata Salazar. El caudillo del Sur".

Sabotaje

La protección contra el sabotaje requiere:

- Una selección rigurosa de los colaboradores.
- Buena administración de los recursos humanos.
- Buenos controles administrativos.
- Buena seguridad física en los ambientes donde están los principales componentes del equipo.

Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.

Medidas que se deben tener muy en cuenta para tratar de evitar las acciones hostiles:

- Ubicar los equipos en lugares más seguros en donde se prevea cualquier contingencia de este tipo.
- Mantener una lista de números telefónicos de las diferentes dependencias policiales a mano y en lugares donde se pueda hacer un llamado de emergencia.
- Siempre habrá de tomarse en cuenta las Políticas de Seguridad en caso como terrorismo y sabotaje. Es importante la medida de ingreso de personas debidamente identificadas, marcación de zonas de acceso restringido, prevención para explosivo, etc.
- Mantener adecuados archivos de reserva (backup)
- Identificar y establecer operaciones críticas prioritarias cuando se planea el respaldo de los servicios y la recuperación de otras actividades.
- Montar procedimientos para remitir registro de almacenamiento de archivos y recuperarlos.

ELABORÓ		REVISÓ Y APROBÓ	
Nombre	JOVANY CARBAJAL MUÑOZ	Nombre	JAVIER HERNADEZ ALVA
Cargo	Programador encargado de Laboratorio Informático de Diseño Industrial	Cargo	JEFE DE AREA DE SISTEMAS



SECRETARÍA DE EDUCACIÓN

SUBSECRETARÍA DE EDUCACIÓN SUPERIOR Y NORMAL

DIRECCIÓN GENERAL DE EDUCACIÓN SUPERIOR

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE CHICOLOAPAN

Camino al Monte s/n, col. Loma de Guadalupe, c.p. 56380, Chicoloapan de Juárez, Estado de México.

Tel.: (0155) 6315 6655.