BACHILLERATO DEL ESTADO DE HIDALGO

EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

BACHILLERATO DEL ESTADO DE HIDALGO

PLAN DE CONTINGENCIA INFORMÁTICO

DIRECCIÓN DE PLANEACIÓN

SUBDIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

BACHILLERATO DEL ESTADO DE HIDALGO

EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

ÍNDICE
CONTENIDO

Introducción	*2*
Finalidad	*3*
Objetivos	3
Identificación de riesgos	5
Resumen de riesgos	7
Implementación del plan	9

1.- INTRODUCCIÓN

A medida que las instituciones se han vuelto cada vez más dependientes de las computadoras, las redes de comunicación y de los sistemas de información para mejorar sus actividades, el Bachillerato del Estado de Hidalgo (BEH), considera importante definir un plan de contingencia informático como un proceso continuo de planeación, desarrollo, pruebas e implementación de procedimientos de recuperación en caso de una posible contingencia que pueda presentarse en la Institución.

Estas acciones buscan asegurar la reanudación eficiente y efectiva de los servicios tanto de hardware, software y redes de comunicación en el menor tiempo e impacto posible.

A medida que la tecnología ha ido evolucionando y con ella, la envergadura del Hardware, Software y Redes de Comunicación de la Institución, la seguridad en el entorno Informático, se ha convertido en la preocupación más importante de la Subdirección de TIC's.

Es por eso que en el presente documento se pretende ayudar a comprender mejor la problemática implícita de los equipos de Cómputo, los Sistemas de Información y las Redes de Comunicación, así como la seguridad que se le pondrá a cada una de ellas, para la recuperación de una posible contingencia.

¿Por qué de este documento?

Un plan de contingencia informático es esencial para cualquier organización que dependa de tecnologías de la información, ya que garantiza la continuidad operativa ante eventos adversos.

2.- FINALIDAD

Garantizar la continuidad de los servicios Informáticos, Sistemas de Información y Redes de Comunicación del Bachillerato del Estado de Hidalgo, a fin de que se restablezcan en el menor tiempo posible, en caso de que ocurra alguna eventualidad que interrumpa su funcionamiento.

3.- OBJETIVOS

3.1 Objetivo General

Establecer los principios básicos para garantizar la operatividad de los servicios y/o procesos en las tecnologías de la información y Redes de Comunicación de mayor prioridad del Bachillerato del Estado de Hidalgo, ante la eventual presencia de siniestros que puedan paralizar parcial o totalmente alguna actividad.

3.2 Objetivos Específicos

3.2.1 Identificar y Analizar los riesgos posibles que puedan afectar las operaciones, procesos y servicios de Hardware, Software y Redes de Comunicación de la Institución.

3.2.2 Definir las Actividades de planeación, preparación, entrenamiento y ejecución de las tareas destinadas a proteger los servicios informáticos, Sistemas de Información y Redes de Comunicación contra daños por fenómenos Humanos o naturales.

3.2.3 Organizar y capacitar al personal técnico para afrontar adecuadamente las contingencias que puedan presentarse.

4.- IDENTIFICACIÓN DE RIESGOS

En ésta etapa y basándose en una evaluación cualitativa, se ha realizado el análisis de los diferentes tipos de riesgos en los cuales está expuesta la Dirección General de Bachillerato del Estado de Hid¡3lgo.

4.1 Activos prioritarios.

4.1.1 Sistemas Informáticos, Bases de Datos, Documentación.

4.1.2 Equipos de Cómputo (Servidores, Computadoras, Escaners, Impresoras).

4.1.3 Redes y equipos de Comunicación.

4.1.4 Software de Aplicación y copias de Respaldo.

4.2 Tipos de riesgos en la Seguridad Informática.

4.2.1 Terremotos

Este es un riesgo por desastre natural, donde el Bachillerato del Estado de Hidalgo no está exento a que pueda suceder, por lo cual se debe tener alguna medida de respaldo de la información.

4.2.2 Inundaciones

Otro desastre natural donde una fuerte precipitación por lluvias hiciera que se colapsen ductos de desagüe en las oficinas, se podrían inundar documentos y equipos Informáticos.

4.2.3 Fallo en el Electricidad

Provocado por alguna falla eléctrica para el uso de los equipos informáticos.

4.2.4 Incendios.

Las oficinas del Bachillerato del Estado de Hidalgo no están exentas a que suceda una catástrofe como este tipo y la cual provocaría pérdidas totales de documentación y Equipos Informáticos.

4.2.5 Fallas de los Servidores(hardware)

Se tiene un plan de mantenimiento de equipos, pero no se está exento de que los equipos fallen y se pueda perder información.

4.2.6 Errores Humanos

El nivel de preparación de los empleados para afrontar las equivocaciones y cómo afrontarlos.

4.2.7 Falla de Redes y Equipos de Comunicación.

Pérdidas totales o parciales de comunicación entre Usuarios y Servidores, por las cuales los procesos pueden verse interrumpidos hasta encontrar la falla y la solución.

4.2.8 Virus

Pérdidas o daño de información por infección de virus.

4.2.9 Falla de Software

Se produce cuando no se hace un análisis de sistemas en la etapa de construcción.

4.3 Probabilidad de que ocurra el riesgo

RIESGO	PROBABILIDAD
Terremoto	Baja
Inundaciones	Muy Baja
Fallo en la Electricidad	Media
Incendios	Alta
Falla de los Servidores	Media
Errores humanos	Media
Falla de Redes y Equipos de Comunicación	Media
Virus	Alta
Falla de Software	Media

5. RESUMEN DE RIESGOS

El servicio de internet se proporcionará a los usuarios tomando en consideración los tipos de acceso que se describen a continuación.

RIESGO	CONSECUENCIAS	MEDIO DE CONTROL	PLAN DE CONTINGENCIA
Terremoto	Interrupción de Servidores, Internet, Red Local, Equipos de Computo	Activar plan de contingencia: Terremoto	Tener un respaldo espejo de los Sistemas de Información en otro espacio físico fuera de la oficina o en la NUBE
Inundaciones	Interrupción de Servidores, Internet, Red Local y Equipos de Computo	Activar plan de contingencia: Inundaciones	Tener un respaldo espejo de los Sistemas de Información en otro espacio físico fuera de la oficina o en la NUBE
Fallo en la Electricidad	Interrupción de Servidores, Internet, Red Local y Equipos de Computo	Activar plan de contingencia: Falla de Electricidad	Entra el respaldo de Celdas Solares o tener una planta de luz disponible para estos casos. (Situación deseable)
Incendios	Interrupción de Servidores, Internet, Red Local y Equipos de Cómputo, posible pérdida de documentación	Activar plan de contingencia: Incendios	Capacitar al personal en el uso de extinguidores y Tener un respaldo espejo de los Sistemas de Información en otro espacio físico fuera de la oficina o en la NUBE
Falla de los Servidores	Interrupción de Servidores por hardware dañado o carga de Software	Activar plan de contingencia: Falla de Servidores	Capacitación constante al personal de la Subdirección de TIC's para mantenimientos correctivos y preventivos tanto de software o de hardware, tener un respaldo espejo en la NUBE
Errores Humanos	Interrupción de Servidores, Internet, Red Local y Equipos deComputo	Activar plan de contingencia: Errores Humanos	Capacitación constante al personal de la Subdirección de TIC's en hardware de Servidores y redes y programación de Software

El servicio de internet se proporcionará a los usuarios tomando en consideración los tipos de acceso que se describen a continuación.

RIESGO	CONSECUENCIAS	MEDIO DE CONTROL	PLAN DE CONTINGENCIA
Falla de Redes y Equipos de Comunicación	Interrupción de Servidores, Internet, Red Local y Equipos deComputo	Activar plan de contingencia: Falla de Redes y Equipo de Comunicación	Capacitación constante al personal de la Subdirección de TIC's en hardware de Servidores y redes y programación de Software
Virus	Pérdida de Información en los Sistemas Informáticos por robo	Activar plan de contingencia: Virus	Instalación de Antivirus que contrarresten los virus troyanos, Malware, gusanos, Spyware y tener un respaldo espejo de los Sistemas de Información en otro espacio físico fuera de la oficina o en la NUBE
Falla de Software	Pérdida de Información	Activar plan de contingencia: Falla de Software	Tener un respaldo espejo de los Sistemas de Información en la NUBE

6.- IMPLEMENTACIÓN DEL PLAN

6.1 De Prevención

Acciones preventivas a ejecutar, antes que ocurra un siniestro o desastre. Su finalidad es evitar la materialización y en caso ocurriese, tener todos los medios requeridos para realizar la recuperación de los servicios de tecnologías de la información y comunicación, en el menor tiempo posible.

- Monitorear la red y definir medidas preventivas para minimizar o evitar las contingencias.
- Preparar planos de la topología, tener equipos de repuestos de la red, herramientas necesarias todo esto en lugar de fácil acceso.
- Ejecutar y verificar las tareas de copias de respaldo (backup).
- Llevar un control detallado del mantenimiento realizado a cada equipo.
- Elaborar informes técnicos de conformidad, luego de cada mantenimiento efectuado, así como elaborar informes periódicos del funcionamiento.
- Monitorear la red y definir medidas preventivas para minimizar o evitar las contingencias.
- Realizar las pruebas previas de recuperación.
- Coordinar acciones de mantenimiento de sistemas de información existentes asegurando el cumplimiento del ciclo de vida de software.
- Coordinar y verificar que se realicen las copias de respaldo de las fuentes de los aplicativos informáticos existentes en un ambiente adecuado.
- Soporte y mantenimiento de los sistemas y aplicativos instalados en la entidad.
- Documentación, consolidación y validación de los manuales de los sistemas en producción.
- Realizar periódicamente las pruebas de restauración de las fuentes de los sistemas de información en producción de la entidad.
- Soporte y mantenimiento de los sistemas y aplicativos instalados en la entidad.
- Realizar copias de respaldo de las bases de datos de los aplicativos y sistemas de la entidad.
- Acopiar las copias de respaldo y clasificarlas por tipo de motor de base de datos, aplicativos y sistemas.
- Realizar las pruebas de restauración de bases de datos.

6.2 De emergencia

Acciones requeridas durante la materialización del siniestro o desastre. Su finalidad es mitigar el impacto que puedan tener sobre los equipos tecnológicos y la información, procurando salvaguardar su pérdida o deterioro.

- Ejecutar las acciones de emergencia en los equipos informáticos y componentes instalados.
- Coordinar acciones para la verificación de estado de los sistemas de información alojados en los servidores de aplicaciones.
- Coordinar acciones para verificar el estado de las bases de datosde los sistemas de información.
- Realizar la evaluación de las condiciones de los aplicativos informáticos y sistemas de información durante la emergencia.
- Solicitar los archivos de registro (logs) de los aplicativos informáticos afectados durante la emergencia.
- Realizar la evaluación de las condiciones de los datos y la información almacenada en las diferentes bases de datos, durante la emergencia.

6.3 De restauración

Acciones necesarias luego de que el siniestro o desastre esté controlado. Su finalidad es restituir en el menor tiempo posible el funcionamiento de los equipos tecnológicos y recuperar el estado de los servicios informáticos.

- Debe iniciar el proceso de recuperación de los servicios de tecnología de la información, realizando las pruebas de funcionamiento en los equipos afectados de la infraestructura informática

- Restaurar la información de los equipos afectados de la infraestructura informática que afecten los servicios
- Coordinar acciones para la verificación de estado de los sistemas de información alojados en los servidores de aplicaciones.
- Coordinar el estado de las bases de datos de los sistemas de información.
- Coordinar y monitorear la restauración de aplicativos y ejecución de pruebas para verificación de funcionalidad.
- Verificar el estado de las aplicaciones alojados en los servidores de aplicaciones.
- En caso se quiera desplegar y/o 'reinstalar los aplicativos informáticos y sistemas de información, de lo contrario verificar que se encuentren funcionando correctamente.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los aplicativos informáticos y sistemas de información.
- Verificar el funcionamiento de las bases de datos institucionales.
- Realizar la creación de bases de datos en servidores alternos, en caso de que sea requerido.
- Restaurar las copias de respaldo correspondientes respetando la prioridad establecida para cada escenario.
- Realizar las pruebas de funcionamiento.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los datos e información.



Elías Cornejo Sánchez
Director General
Bachillerato del Estado de Hidalgo

Agosto 2026