TLAXCALA

UNA NUEVA HISTORIA

PLAN DE RECUPERACIÓN DE DESASTRES Y CONTINUIDAD DE LA OPERACIÓN DE LOS SISTEMAS INFORMÁTICOS

CECYTE Tlaxcala

EMSAD Tlaxcala

MAYO 2022

Fecha	Versión	Descripción	Autor
13/05/2022	1.0	Elaboró	**Ing. José Flores Lara** Ingeniero en Sistemas
			Ing. Wendy Hernández Netzahualcoyotl Programador
27/05/2022	1.1	Revisó	**Ing. Javier Huerta Huerta** Director de Informática
27/05/2022	1.2	Autorizó	**Mtro. José Luis Flores Aguilar** Director General

Av. Reforma No. 10, Col. Tlatempan, Apetatitlán, Tlaxcala, Tlax. Tel. 46 89200 (ext. 2418/2016)
@cecytetlaxcala @TlaxcalaEMSaD www.cecytlax.edu.mx

Tabla de Contenido

1. Introducción. 4
1.1 Justificación 5
1.2 Objetivo General. 5
1.3 Objetivos específicos. 5
1.4 Alcance. 6
2. Preparación del Plan de Riesgos. 6
2.1 Inventario Físico. 6
2.2 Inventario de Aplicaciones. 8
2.3 Inventario de Base de Datos. 8
2.4 Inventario de Personal 9
2.5 Inventario de Proveedores 9
2.6 Administración de Servidores. 10
2.7 Respaldos 10
3. Ejecución del plan 18
3.1 Identificación de vulnerabilidades 18
3.2 Identificación de amenazas 23
3.3 Identificación de riesgos 24
3.4 Clasificación de impacto de riesgos. 24
3.5 Clasificación de probabilidad de riesgos. 25
3.6 Matriz de Riesgos 25
4. Procedimiento de acciones de recuperación. 30
4.1 Desastres naturales y humanos. 30
4.2 Actos Criminales 31
5. Proceso de reconstrucción. 32
6. Anexos 35

1. Introducción.

El crecimiento del Colegio de Estudios Científicos y Tecnológicos del Estado de Tlaxcala a lo largo de los últimos años ha forzado los cambios y mejoras en la infraestructura tecnológica, por lo que en la dirección de informática se generó la normatividad, programas y lineamientos que brindan el control de las tecnologías de Información en CECyTE-EMSaD, sin embargo es importante considerar de igual manera, ¿Cómo tener el control de dichas tecnologías después de un desastre?; con "desastre" nos referimos a cualquier suceso que interrumpa la actividad normal del Colegio, por lo que se deben tomar una serie de medidas para reducir con garantías los efectos derivados de su impacto.

Estas medidas se conocen como *recuperación de desastres* ante un eventual fallo de los sistemas informáticos, las cuales se están convirtiendo en uno de los elementos más importantes dentro del ámbito de la seguridad de Tecnologías de la Información, estos eventos pueden referirse tanto a un desastre natural como a un error humano o un fallo del propio sistema a causa de un software malicioso.

Es por ello que en el presente trabajo se muestra un plan de recuperación de desastres de la seguridad de las Tecnologías de la Información en el Colegio de Estudios Científicos y Tecnológicos del Estado de Tlaxcala.

Av. Reforma No. 10, Col. Tlatempan, Apetatitlán, Tlaxcala, Tlax. Tel. 46 89200 (ext. 2418/2016)
@cecytetlaxcala @TlaxcalaEMSaD www.cecytlax.edu.mx

1.1 Justificación

El tener un plan de recuperación de desastres ante un eventual fallo en el Colegio es de vital importancia para garantizar la seguridad, integridad, respaldo y recuperación de la información generada por el personal en la infraestructura tecnológica, siguiendo los procedimientos descritos en este documento para actuar ante la posibilidad de un desastre.

1.2 Objetivo General.

Garantizar la capacidad de respuesta ante un siniestro u otra emergencia que afecte a los sistemas de información, así como reducir al mínimo el impacto en el colegio.

1.3 Objetivos específicos.

- Identificar y analizar riesgos posibles que pueden afectar las operaciones y procesos informáticos del Colegio.
- Documentar los riesgos por niveles de afectación en los sistemas informáticos de la institución.
- Establecer las estrategias adecuadas para asegurar la recuperación de los servicios informáticos.

1.4 Alcance.

La Implementación del Plan de Recuperación de Desastres y de continuidad de la operación de los sistemas informáticos, incluye los elementos referidos a los sistemas de información, equipos, infraestructura, personal y servicios propiedad del Colegio, direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el funcionamiento normal de los servicios informáticos del colegio.

2. Preparación del Plan de Riesgos.

Se debe contar con un listado general del equipamiento, aplicaciones y personal con que cuenta la dirección de informática.

2.1 Inventario Físico.

El equipamiento de hardware que proporciona el Colegio a la dirección se enlista a continuación.

ID	ACTIVO	MARCA	MODELO	NO. SERIE	UBICACIÓN
FCE001	Almacenamiento TeraStation	BUFFALO	3410DN	ND	Dirección de informática
FCE002	Switch Cisco	CISCO	SF300-24	ND	Dirección de informática
FCE003	Computadora Acer	ACER	VX2610	DTVDBAL0062200CA359200	Dirección de informática
FCE004	Servidor DELL	DELL	POWEREDGE R440	ND	Dirección de informática
FCE005	Conmutador Avaya	AVAYA	PI OFFICE 500 V2	12WZ1620034G	Dirección de informática
FCE006	Firewall Fortinet	FORTI	FG300EBDL95012	ND	Dirección de informática
FCE007	Servidor HP	HP	ML310XEON	MX25010058	Dirección de informática
FCE008	Pc DELL	DELL	APTICEL 960	ND	Dirección de informática
FCE009	Computadora PC HP	HP	ELITE DESK	MXL50313UH	Dirección de informática
FCE010	Switch Cisco	CISCO	SF300-24	DNI16190064F	Dirección de informática
FCE011	Switch Cisco	CISCO	SF300-24	DNI161906FR	Dirección de informática
FCE012	Switch Cisco	CISCO	SF300-24	DNI161906D7	Dirección de informática
FCE013	Switch Cisco	CISCO	SF300-24	DNI162003YN	Dirección de informática
FCE014	Switch Cisco	CISCO	SF300-24	DNI16220461	Dirección de informática
FCE015	Switch Cisco	CISCO	SF300-24	DNI16200466	Dirección de informática
FCE016	AP Ubiquiti	UBIQUITI	NSM5	PTO34594027250	Dirección de informática
FCE017	Access Point	SM	SM	ND	Dirección de informática
FCE018	Switch Cisco	CISCO	SF300-24	ND	Dirección de informática
FCE019	Switch Cisco	CISCO	SF-200-48	ND	Dirección de informática
FCE020	Switch Cisco	CISCO	SF300-24	ND	Dirección de informática
FCE021	Respaldo de baterías	APC	ND	ND	Dirección de informática
FCE022	Respaldo de baterías	APC	ND	ND	Dirección de informática
FCE023	Firewall Fortinet	FORTI	ND	ND	Site Direccion EMSaD
FCE024	Switch Cisco	CISCO	ND	ND	Site Direccion EMSaD
FCE025	Switch Cisco	CISCO	ND	ND	Site Direccion EMSaD
FCE026	Respaldo de baterías	ND	ND	ND	Site Direccion EMSaD
FCE027	Respaldo de baterías	ND	ND	ND	Site Direccion EMSaD
FCE045	CPU	HP	ELITE DESK	MXL50313JH	Dirección de informática

Tabla 1 Inventario Físico

2.2 Inventario de Aplicaciones.

El listado de aplicaciones se describe a continuación.

ID	ACTIVO	ID Y HARDWARE CONTENEDOR DEL ACTIVO	
ICE001	Sistema de Inventarios	FCE007	Servidor HP ML310XEON
ICE002	Sistema SACGNET	FCE045	HP ELITE DESK MXL50313JH
ICE003	Sistema de tickets OS	FCE004	Servidor DELL POWEREDGE R440
ICE004	Información administrativa de la dirección de informática	FCE028	All in one DELL VOSTRO 3471 I3-9100
ICE005	Sitio Web	No Aplica	NUBE DE HOSTING
ICE006	Sistema de Reto Cecyte	FCE004	Servidor DELL POWEREDGE R440
ICE007	Sistema de Evaluación: Reto	FCE004	Servidor DELL POWEREDGE R440
ICE008	Sistema de Monitoreo: Pandora FMS	FCE004	Servidor DELL POWEREDGE R440
ICE009	Sistema SIGA	FCE004	Servidor DELL POWEREDGE R440
ICE010	Respaldos de Bases de Datos	FCE001	Almacenamiento TeraStation BUFFALO 3410DN

Tabla 2 Inventario de aplicaciones

2.3 Inventario de Base de Datos.

El listado de bases de datos contenidas en las aplicaciones y hardware que los ejecuta se describe a continuación.

ID	BASE DE DATOS	ID Y HARDWARE DONDE SE ENCUENTRAN	
ICE001	Sistema de Inventarios	FCE007	Servidor HP ML310XEON
ICE002	Sistema SACGNET	FCE045	HP ELITE DESK MXL50313JH
ICE003	Sistema de tickets OS	FCE004	Servidor DELL POWEREDGE R440
NA	Moodle		
ICE006	Sistema de Reto Cecyte		
ICE007	Sistema de Evaluación: Reto		
ICE009	Sistema SIGA		
ICE010	Respaldos de Bases de Datos	FCE001	Almacenamiento TeraStation BUFFALO 3410DN

Tabla 3. Inventario de Base de Datos.

2.4 Inventario de Personal

La dirección de Informática cuenta con los siguientes operativos:

ID	ACTIVO
HCE001	Director de Informática
HCE002	Jefe de Oficina
HCE003	Ingeniero en Sistemas
HCE004	Programador 1
HCE005	Programador 2
HCE006	Programador 3
HCE007	Programador 4
HCE008	Analista Especializado 1
HCE009	Analista Especializado 2

Tabla 4. Inventario de Personal

2.5 Inventario de Proveedores

Los proveedores de los servicios solicitados en la dirección de informática se enlistan a continuación:

ID	ACTIVO
HCE010	Blacom
HCE011	Telmex
HCE012	CFE

Tabla 5. Inventario de Proveedores

2.6 Administración de Servidores.

Se administra y mantiene funcionando en óptimas condiciones los siguientes servidores:

- Servidor DELL PowerEdge R440 como plataforma de virtualización.
- Servidor HP ML310XEON - sistema de inventarios.
- CPU HP ELITE DESK MXL50313JH - sistema SACGNET.

Tipo	Marca	Modelo	ID	Sistema Operativo	Ubicación
Servidor	DELL	PowerEdge R440	FCE004	Debian 10	Site Dirección General
Servidor	HP	EliteDesk	FCE009	Windows 10	Site Dirección General
Servidor	HP	ProLiant ML310e Gen8 v2	FCE007	Windows 10	Site Dirección General

Tabla 6. Administración de servidores

2.7 Respaldos

Un respaldo es una copia de la información que las áreas del Colegio generan, utilizan y actualizan a lo largo del tiempo; nos referimos a las copias de seguridad que se llevan a cabo en el software de aplicación.

El objetivo de un respaldo es garantizar la recuperación de la información, en caso de que haya sido eliminada, dañada o alterada al presentarse alguna contingencia.

Normalmente, los respaldos se llevan a cabo en unidades de almacenamiento secundario, como discos duros externos, memorias flash, en la nube (Internet) o en otros equipos de cómputo, locales o remotos.

Es una buena práctica establecer políticas institucionales relacionadas con la creación de respaldos, pues el tiempo que hay entre la posible pérdida de información y su recuperación puede ser determinante para la supervivencia de una organización, es por ello que organizamos los respaldos de la siguiente manera:

- Servidores.
  - Periodicidad: bajo demanda.
  - Método de respaldo: manual.
  - Descripción: Se respaldan los archivos de configuración antes de hacer alguna modificación al sistema y se almacenan en una unidad externa.
- Servidores Virtuales
  - Periodicidad: después de cambios en su configuración.
  - Método de respaldo: Manual
  - Se respaldan las máquinas virtuales y se almacenan en una NAS (Buffalo TS3210D 4TB) y se mantienen los tres últimos respaldos sin demás históricos.

ID ACTIVO	Servidor Virtual	Sistema Operativo
FCE004	Proxy Inverso	GNU/Linux Debian 10
	Ticket	GNU/Linux Ubuntu 20
	Retocecyte	GNU/Linux Ubuntu 20
	Examen de admisión	GNU/Linux Ubuntu 20
	Servidor web de prueba	GNU/Linux Debian 10
	Moodle	GNU/Linux Ubuntu 20
	Siga	GNU/Linux Debian 10
	DBSIGA	Windows server 2008

Tabla 7. Servidores virtuales

- Aplicaciones web.
  - Periodicidad: Después de una actualización.
  - Método de respaldo: Clonación

Aplicación	Aplicativo	Nota
INVEC	Genero Fourjs	Software con licenciamiento temporal
Sacgnet	Java EE	Se cuenta con discos de instalación.
Sistema de tickets OS	PHP	Software libre
Sistema de Reto Cecyte	Java	Periodo de desarrollo liberado
Sistema de Evaluación: Reto	Java	Periodo de desarrollo liberado
Sistema SIGA	Java	Periodo de desarrollo liberado

Tabla 8. Aplicaciones WEB

- Bases de datos.
  - Periodicidad: Semanal
  - Método de respaldo: manual
  - Se respaldan las bases de datos MySQL en memoria flash y se almacenan los históricos en unidades de almacenamiento en la nube de Google drive.

ID	Base de datos	Tipo de base de datos
ICE001	Sistema de Inventarios	SQL
ICE002	Sistema SACGNET	SQL

ICE003	Sistema de ticket OS	MySQL
FCE004	Moodle	MySQL
ICE006	Sistema de Reto Cecyte	MySQL
ICE007	Sistema de Evaluación Reto	MySQL
ICE009	SIGA	SQL
ICE010	WWW	MySQL

Tabla 9. Bases de datos

- Procedimiento:
  - Iniciar sesión en el servidor que aloja la base de datos de la que desea realizar una copia de seguridad.
  - Abrir Microsoft SQL Server Management Studio.
  - En la barra de navegación izquierda, expandir Bases de datos.
  - Pulsar con el botón derecho del ratón en la base de datos de la que desea hacer una copia de seguridad y, a continuación, pulse Tareas > Copia de seguridad.
  - Revisar los detalles de la copia de seguridad y, a continuación, pulse Agregar para crear la copia de seguridad.
  - Seleccionar el path donde guardará la copia de seguridad (USB o nube) y nombrar el archivo .bak, dar click en Aceptar.
  - Al completar el 100% de la copia de seguridad dar click en Aceptar.
  - Respaldar la copia de seguridad en un equipo de cómputo independiente al sistema.

Flujogramas de respaldos:

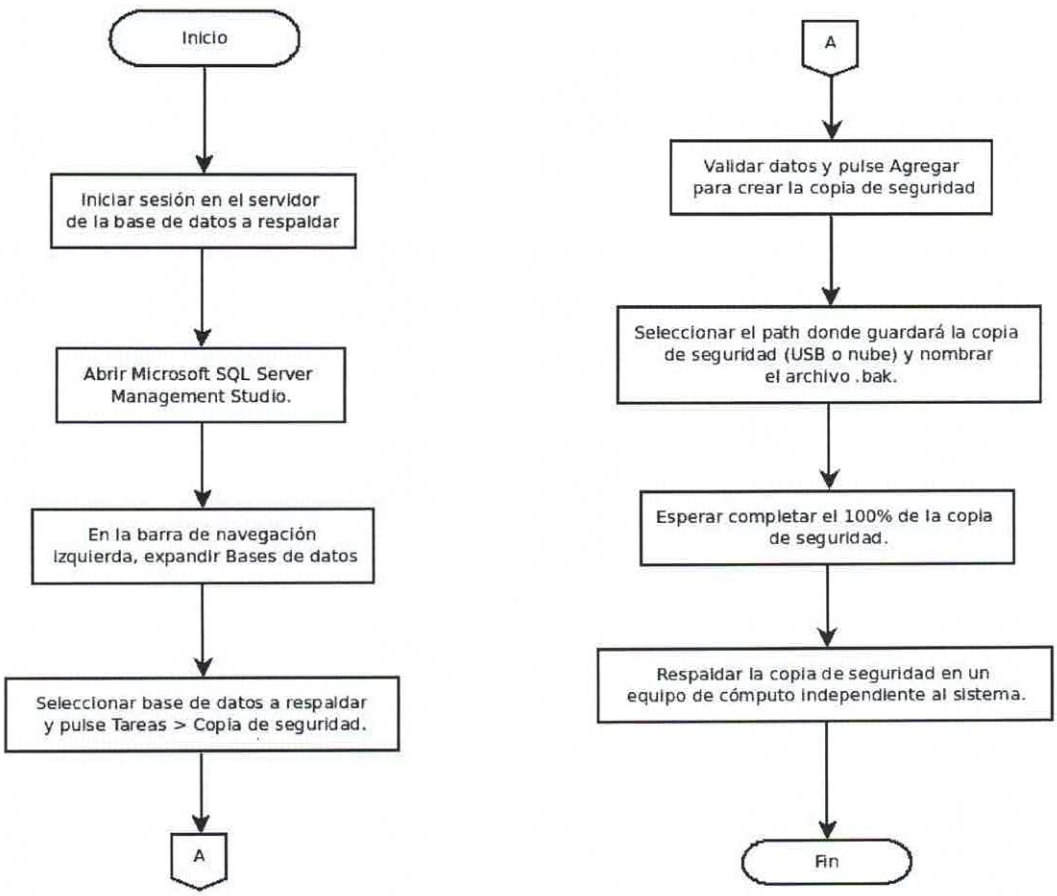

Imagen 1. Respaldo Manual

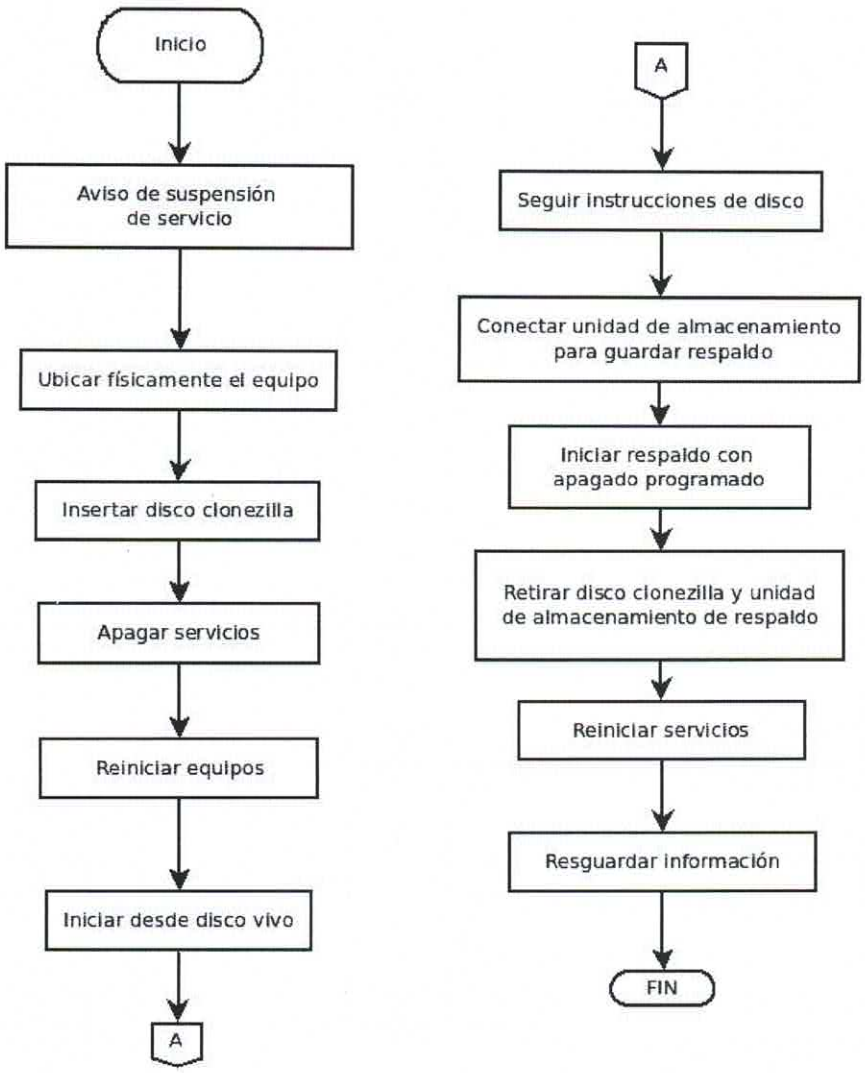

Imagen 2. Respaldo por clonación

Imagen 3. Respaldo Máquinas Virtuales

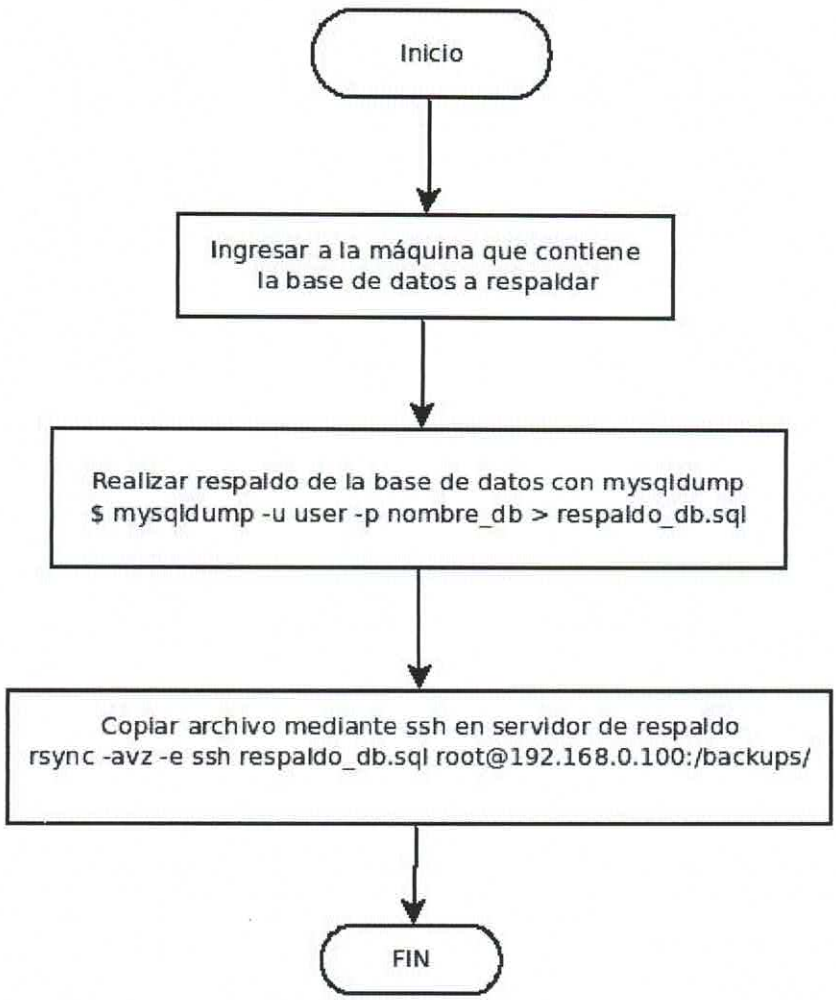

Imagen 4. Respaldo MySQL

3. Ejecución del plan

3.1 Identificación de vulnerabilidades

Vulnerabilidad, es un punto débil en la seguridad de un sistema informático, la presencia de una, incrementa la probabilidad de que una amenaza impacte en los activos.

ID	ACTIVO	VULNERABILIDAD
ICE001	Sistema de Inventarios	No se registran las modificaciones aplicadas
		Falta de programación de mantenimiento
		Permitir que una persona ajena acceda al dispositivo
		Falla eléctrica
		Sin soporte técnico
		Sin respaldos automatizados
		Sin licenciamiento
ICE002	Sistema SACGNET	Falla eléctrica
		Permitir que una persona ajena acceda al dispositivo
		Sin respaldos automatizados
		Sin protección contra borrado accidental
ICE003	Sistema de tickets OS	Permitir que una persona ajena acceda al dispositivo
ICE004	Información administrativa de la dirección de informática	Sin protección contra borrado accidental
ICE005	Sitio Web	Respaldos desactualizados
ICE006	Sistema de Reto Cecyte	Permitir que una persona ajena acceda al dispositivo
		Falta de programación de mantenimiento
		Sin soporte técnico
		Sin protección contra borrado accidental

ID	ACTIVO	VULNERABILIDAD
ICE007	Sistema de Evaluación: Reto	Falta de programación de mantenimiento
		Sin soporte técnico
		Sin protección contra borrado accidental
ICE008	Sistema de Monitoreo: Pandora FMS	Permitir que una persona ajena acceda al dispositivo
ICE009	Sistema SIGA	Permitir que una persona ajena acceda al dispositivo
		Varios usuarios pueden acceder a él.
		Falta de programación de mantenimiento
		Sin soporte técnico
ICE010	Respaldos de Bases de Datos	Respaldos guardados en el mismo equipo que contiene el sistema
ICE011	Manual DRP	Sin corroboración jurídica
ICE012	Plan de Trabajo	Sin corroboración jurídica
ICE013	Normativa infraestructura TIC'S	Sin corroboración jurídica
ICE014	Lineamientos Seguridad 2022 TICS	Sin corroboración jurídica
ICE015	Manual de Organización de la Dirección de Informática	Sin corroboración jurídica
ICE016	Normativa Correo Institucional	Sin corroboración jurídica

Tabla 10. Vulnerabilidades en activos de información

ID	ACTIVO	VULNERABILIDAD
FCE001	Almacenamiento TeraStation	Permitir que una persona ajena acceda al dispositivo
		Daños eléctricos
FCE002	Switch Cisco	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo
FCE003	Computadora Acer	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo
FCE004	Servidor DELL	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo
FCE005	Conmutador Avaya	Daños eléctricos
		Sin soporte técnico de fabricante
		Permitir que una persona ajena acceda al dispositivo
FCE006	Firewall Fortinet	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo
FCE007	Servidor HP	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo
FCE008	Pc DELL	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo
FCE009	Computadora PC HP	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo
FCE010	Switch Cisco	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo
FCE011	Switch Cisco	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo
FCE012	Switch Cisco	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo
FCE013	Switch Cisco	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo
FCE014	Switch Cisco	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo

ID	ACTIVO	VULNERABILIDAD
FCE015	Switch Cisco	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo
FCE016	AP Ubiquiti	Daños eléctricos
FCE017	Access Point	Daños eléctricos
FCE018	Switch Cisco	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo
FCE019	Switch Cisco	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo
FCE020	Switch Cisco	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo
FCE021	Respaldo de baterías	Daños eléctricos
FCE022	Respaldo de baterías	Daños eléctricos
FCE023	Firewall Fortinet	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo
FCE024	Switch Cisco	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo
FCE025	Switch Cisco	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo
FCE026	Respaldo de baterías	Daños eléctricos
FCE027	Respaldo de baterías	Daños eléctricos
FCE045	CPU	Daños eléctricos
		Permitir que una persona ajena acceda al dispositivo

Tabla 11. Vulnerabilidades en activos físicos

ID	ACTIVO	VULNERABILIDAD
HCE001	Director de Informática	Sin programa de capacitación
HCE002	Jefe de Oficina	Sin programa de capacitación
HCE003	Ingeniero en Sistemas	Sin programa de capacitación
HCE004	Programador 1	Sin programa de capacitación
HCE005	Programador 2	Sin programa de capacitación
HCE006	Programador 3	Sin programa de capacitación
HCE007	Programador 4	Sin programa de capacitación
HCE008	Analista Especializado 1	Sin programa de capacitación
HCE009	Analista Especializado 2	Sin programa de capacitación

Tabla 12. Vulnerabilidades en activos humanos

3.2 Identificación de amenazas

Amenaza es un evento que puede producir daños en los activos del sistema, puede ser provocada por usuarios internos o ajenos a la organización.

NEGLIGENCIAS Y MALAS DECISIONES	ACTOS CRIMINALES	INCIDENTES DE ORIGEN FÍSICO
Falta de capacitación y sensibilización sobre riesgos	Robo físico	Incendios, sismos, desastres naturales
Mal manejo de sistemas y herramientas	Espionaje digital	Polvo
Uso de software no licenciado o no autorizado	Allanamiento Físico	Fallas eléctricas
Eliminación accidental de datos		Fallas circunstanciales en los sistemas
Falta de definición de privilegios y restricciones de personal		
Falta de normas y reglas claras (Ausencia de documentación)		

Tabla 13. Clasificación de amenazas

3.3 Identificación de riesgos

1. Criminalidad
   - Robo
   - Allanamiento / Accesos no autorizados
2. Naturales o Físicas
   - Sismos
   - Incendios
   - Eléctrico
3. Negligencia
   - Mal manejo
   - Datos incorrectos

3.4 Clasificación de impacto de riesgos.

IMPACTO	DESCRIPCIÓN	FACTOR
Insignificante	Consecuencias que no afectan significativamente el funcionamiento del área; sin pérdidas.	1
Marginal	Consecuencias que afectan de forma leve; pérdidas menores.	2
Importante	Consecuencias que afectan parcialmente al área; pérdidas moderadas.	3
Crítica	Consecuencias que afectan de forma grave al área; pérdidas moderadas a mayores.	4

Tabla 14. Clasificación de impacto

3.5 Clasificación de probabilidad de riesgos.

PROBABILIDAD	DESCRIPCIÓN	FACTOR
Imposible	Muy baja posibilidad de ocurrencia, nunca ha ocurrido un accidente.	1
Remoto	Limitada posibilidad de ocurrencia, ha ocurrido una vez al año.	2
Ocasional	Ha ocurrido varias veces, ha ocurrido una vez al mes.	3
Frecuente	Alta posibilidad de ocurrencia, Ocurre una vez a la semana.	4

Tabla 15. Clasificación de Probabilidad de amenaza

3.6 Matriz de Riesgos

Cálculo de riesgos

Se maneja la ecuación universal de riesgo:

Riesgo = Probabilidad x Impacto

El valor obtenido será colocado en la Matriz de Valoración.

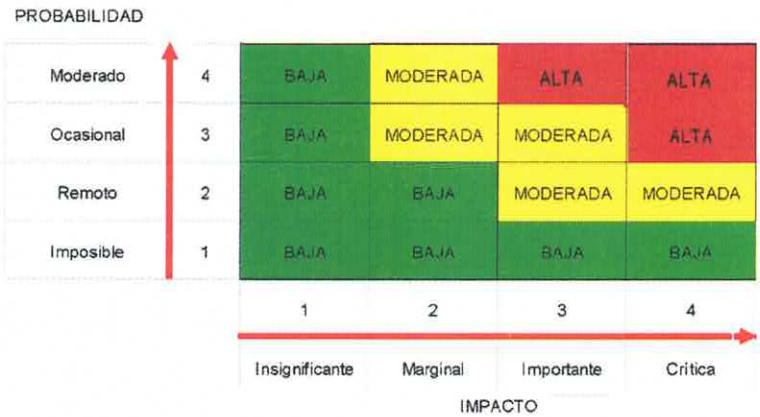

Imagen 5. Matriz de riesgos

Consideraciones:

- Si el nivel de riesgo estimado es bajo, puede ser aceptado, mientras que si es alto deben tomarse medidas para mitigarlo, prevenirlo o transferirlo.

Transferencia del Riesgo:

- Si la dirección no cuenta con la capacidad para implementar las medidas de seguridad necesaria, contrata los servicios de un proveedor especializado en seguridad informática que se encargue de hacerlo.
- La prioridad es la seguridad de la información.

3.7 Identificación de riesgos.

Clasificación de riesgos de Información

	AMENAZAS	CRIMINALIDAD		FISICAS			NEGLIGENCIA	
		ROBO	ALLANAMIENTO	INCENDIO	ELÉCTRICO	SISMO	MAL MANEJO	DATOS INCORRECTOS
INFORMACION	MAGNITUD DEL IMPACTO	PROBABILIDAD DE OCURRENCIA DE AMENAZA: 1. Nunca a ocurrido un accidente 2. Ha ocurrido una vez en el ultimo año 3. Ocurrido una vez al mes 4.Ocurren una vez a la semana.						
		1	1	1	3	2	3	2
Sistema de Inventarios	4	4	4	4	12	8	12	8
Sistema SACGNET	4	4	4	4	12	8	12	8
Sistema de tickets OS	3	3	3	3	9	6	9	6
Información administrativa de la dirección de informática	3	3	3	3	9	6	9	6
Sitio Web	4	4	4	4	12	8	12	8
Sistema de Reto Cecyte	4	4	4	4	12	8	12	8
Sistema de Evaluación: Reto	4	4	4	4	12	8	12	8
Sistema de Monitoreo: Pandora FMS	3	3	3	3	9	6	9	6
Sistema SIGA	4	4	4	4	12	8	12	8
Respaldos de Bases de Datos	4	4	4	4	12	8	12	8
Manual DRP	3	3	3	3	9	6	9	6
Plan de Trabajo	3	3	3	3	9	6	9	6
Normativa infraestructura TIC'S	3	3	3	3	9	6	9	6
Lineamientos Seguridad 2022 TICS	3	3	3	3	9	6	9	6
Manual de Organización de la Dirección de Informática	3	3	3	3	9	6	9	6
Normativa Correo Institucional	3	3	3	3	9	6	9	6

Clasificación de riesgos de activos físicos

	AMENAZAS	CRIMINALIDAD		FISICAS			NEGLIGENCIA	
		ROBO	ALLANAMIENTO	INCENDIO	ELÉCTRICO	SISMO	MAL MANEJO	DATOS INCORRECTOS
INFRAESTRUCTURA / FISICOS	MAGNITUD DEL IMPACTO	PROBABILIDAD DE OCURRENCIA DE AMENAZA: 1. Nunca a ocurrido un accidente 2. Ha ocurrido una vez en el ultimo año 3. Ocurrido una vez al mes 4.Ocurren una vez a la semana.						
		1	1	1	3	2	3	2
Almacenamiento TeraStation	4	4	4	4	12	8	12	8
Switch Cisco	3	3	3	3	9	6	9	6
Computadora Acer	3	3	3	3	9	6	9	6
Servidor DELL	4	4	4	4	12	8	12	8
Conmutador Avaya	4	4	4	4	12	8	12	8
Firewall Fortinet	4	4	4	4	12	8	12	8
Servidor HP	4	4	4	4	12	8	12	8
Pc DELL	4	4	4	4	12	8	12	8
Computadora PC HP	4	4	4	4	12	8	12	8
Switch Cisco	3	3	3	3	9	6	9	6
Switch Cisco	3	3	3	3	9	6	9	6
Switch Cisco	3	3	3	3	9	6	9	6
Switch Cisco	3	3	3	3	9	6	9	6
Switch Cisco	3	3	3	3	9	6	9	6
Switch Cisco	3	3	3	3	9	6	9	6
AP Ubiquiti	3	3	3	3	9	6	9	6
Access Point	3	3	3	3	9	6	9	6
Switch Cisco	3	3	3	3	9	6	9	6
Switch Cisco	3	3	3	3	9	6	9	6
Switch Cisco	3	3	3	3	9	6	9	6
Respaldo de baterias	4	4	4	4	12	8	12	8
Respaldo de baterias	4	4	4	4	12	8	12	8
Firewall Fortinet	4	4	4	4	12	8	12	8
Switch Cisco	3	3	3	3	9	6	9	6
Switch Cisco	3	3	3	3	9	6	9	6
Respaldo de baterias	4	4	4	4	12	8	12	8
Respaldo de baterias	4	4	4	4	12	8	12	8
CPU	4	4	4	4	12	8	12	8

Clasificación de riesgos de activos humanos

	AMENAZAS	CRIMINALIDAD		FISICAS			NEGLIGENCIA	
		ROBO	ALLANAMIENTO	INCENDIO	ELÉCTRICO	SISMO	MAL MANEJO	DATOS INCORRECTOS
HUMANOS	MAGNITUD DEL IMPACTO	PROBABILIDAD DE OCURRENCIA DE AMENAZA: 1. Nunca a ocurrido un accidente 2. Ha ocurrido una vez en el ultimo año 3. Ocurrido una vez al mes 4.Ocurren una vez a la semana.						
		1	1	1	3	2	3	2
Director de informática	4	4	4	4	12	8	12	8
Jefe de Oficina	4	4	4	4	12	8	12	8
Ingeniero en Sistemas	4	4	4	4	12	8	12	8
Programador 1	4	4	4	4	12	8	12	8
Programador 2	4	4	4	4	12	8	12	8
Programador 3	4	4	4	4	12	8	12	8
Programador 4	4	4	4	4	12	8	12	8
Analista Especializado 1	4	4	4	4	12	8	12	8
Analista Especializado 2	4	4	4	4	12	8	12	8

4. Procedimiento de acciones de recuperación.

4.1 Desastres naturales y humanos.

A continuación, se muestran las amenazas y procedimientos en caso de que se inhabilite la operación continua de los servicios informáticos

AMENAZAS	PROCEDIMIENTO	RESPONSABLE
FÍSICAS: Fallas eléctricas, Sismos, Incendios.	Se cuenta con infraestructura de soporte compatible para la migración entre el site principal (Dirección General) y el site secundario (Coordinación Emsad) Se cargan los respaldos de las máquinas virtuales al site secundario para evitar la falta de continuidad en los servicios. Se carga la información correspondiente al servicio (clones de aplicación, respaldo de bases de datos) Redirección de IP públicas.	Ing. Javier Huerta Huerta Ing. José Flores Lara Ing. Wendy Hernández Netzahualcoyotl Ing. Edgar Isaac Flores Medrano
NEGLIGENCIA	Desinstalar software no autorizado o sin licencia. Recuperar en respaldos la información eliminada. Solicitar capacitaciones de actualización al personal. Actualizar normas y lineamientos. Definir privilegios y restricciones.	Ing. Javier Huerta Huerta Todo el personal operativo de la dirección de informática.

Tabla 16. Amenazas

4.2 Actos Criminales

Para evitar espionaje digital o infiltración digital:

- Se utilizan Servidores Virtuales basados en GNU-Linux los cuales están exentos de ataques por virus.
- Se configuran firewalls para restringir el acceso por puertos que no estén autorizados o que busquen explotar vulnerabilidades
- Se escanean periódicamente los sistemas de archivos en busca de virus y/o malware como medida preventiva.
- Todas las computadoras del colegio tienen activado antivirus con licencia y actualizado (Bitdefender y Microsoft Defender).
- En caso de alguna anomalía en el funcionamiento del servidor, se manda a cuarentena el servidor virtual y se carga un respaldo anterior el cual no presenta problemas.
    - Si la máquina virtual ha sido comprometida, respaldar la información, archivar para su análisis y eliminarla del servidor de virtualización.

En caso de robo físico:

- Se carga el clon de respaldo de las aplicaciones web y los respaldos de las bases de datos en un nuevo equipo de cómputo.
- Se configuran las rutas de acceso a servidores que sean necesarias.

5. Proceso de reconstrucción.

Se deberá seguir los siguientes pasos:

- Contactar y organizar al equipo de recuperación en caso de siniestro.

PERSONAL RESPONSABLE DE CONTINUIDAD DE TRABAJO		
NOMBRE	**CARGO**	**TELÉFONO**
Ing. Javier Huerta Huerta	Director de Informática	2462443047
Ing. José Flores Lara	Administrador de servidores físicos y virtuales del colegio.	2461341958
Ing. René Barragán	Ingeniero de soporte técnico de los equipos de las tecnologías de la información y comunicación.	2464690198
Ing. Edwin Juárez Núñez	Soporte Técnico de Sistemas de Información Administrativos	2461851943
Lic. Jesús Vázquez Pérez	Responsable del Programa Anual de Mantenimiento Preventivo y Correctivo.	2464593751
Ing. Alíen Corona Pérez	Ingeniero de soporte en los equipos de TICS.	2462986962
Ing. Edgar Flores Medrano	Responsable de dominios cecytlax.edu.mx.	2211674788
Ing. Wendy Hernández Netzahualcoyotl	Responsable de ciberseguridad.	2461423705
CP. Martín Ortiz Juárez	Administrador de mesa de ayuda de soporte técnico	2464574295

Tabla 17. Directorio de personal

- Contactar a los proveedores de servicios según sea el siniestro.

PROVEEDORES DE SERVICIOS 2022			
EMPRESA	**CONTACTO**	**CARGO**	**TELÉFONO**
BLACOM	Carlos Arturo Padilla Castillo	Representante legal de telecomunicaciones autónomas sin límite SA de CV (Blacom)	222 6413505
CFE	Alejandra García	Encargada de cobranza centralizada	5 16 28 5 16 25 2222
TELMEX	Jose Ramón Felipe Sánchez García	Gerente de mercado empresarial área Tlaxcala	2464623123

Tabla 18. Directorio de proveedores

- Notificar a los usuarios de la interrupción de los servicios.
- Establecer como centro de operaciones alterno el site de la coordinación de EMSaD, en donde se encuentran los respaldos de los servicios informáticos.
- Alquilar o comprar equipo en caso necesario.
- Identificar el grado del siniestro.

- Solicitar al director de informática el sobre contenedor de accesos y contraseñas de activos de la dirección de informática en caso de ser necesario.
- Cargar los servicios necesarios en equipos de repuesto, así como los respaldos de las bases de datos correspondientes.
- Elaborar por escrito el procedimiento llevado a cabo de cada una de las tareas realizadas por el equipo.

Av. Reforma No. 10, Col. Tlatempan, Apetatitlán, Tlaxcala, Tlax. Tel. 46 89200 (ext. 2418/2016)
@cecytetlaxcala @TlaxcalaEMSaD www.cecytlax.edu.mx

6. Anexos

ANEXO 1.- Mantenimiento Preventivo.

TLAXCALA UNA NUEVA HISTORIA EDUCACIÓN SEPE USET CECyTE EMSaD

COLEGIO DE ESTUDIOS CIENTÍFICOS Y TECNOLÓGICOS DEL ESTADO DE TLAXCALA
DIRECCIÓN DE INFORMÁTICA

REPORTE DE MANTENIMIENTO		
Fecha	Realizo	Área o plantel
30/07/21	José Flores Lara	Dirección de Informática
Descripción del equipo		
Equipo	Marca y Modelo	Datos Técnicos
Conmutador VoIP	AVAYA IP office 500 V2	384 extensiones 204 enlaces troncales 240 canales
Diagnostico del equipo		
Falla	causa	solución
No se activa la contestadora para llamadas entrantes.	Después de la revisión del equipo avaya se encuentra falla de tarjeta SD	Se realiza arranque con flash del equipo y se realizan configuraciones nuevas para contestadora automática y grabación de mensaje de bienvenida
Observaciones		
No se tiene conexión con correo de voz Voice Mail Pro.		
Nombre y firma responsable del servicio		Nombre y Firma de conformidad del usuario
José Flores Lara		TLAXCALA Informática COLEGIO DE ESTUDIOS CIENTÍFICOS Y TECNOLÓGICOS DEL ESTADO DIRECCION DE INFORMÁTICA

Av. Reforma No. 10, Col. Tlatempan, Apetatitlán, Tlaxcala, Tlax. Tel. 46 89200 (ext. 2016)
@cecytetlaxcala @TlaxcalaEMSaD www.cecytlax.edu.mx

TLAXCALA UNA NUEVA HISTORIA EDUCACIÓN SEPE USET CECyTE EMSaD

COLEGIO DE ESTUDIOS CIENTÍFICOS Y TECNOLÓGICOS DEL ESTADO DE TLAXCALA

DIRECCIÓN DE INFORMÁTICA

REPORTE DE MANTENIMIENTO		
Fecha	Realizo	Área o plantel
19/07/21	José Flores Lara	Dirección de Informática
Descripción del equipo		
Equipo	Marca y Modelo	Datos Técnicos
Conmutador VoIP	AVAYA IP office 500 V2	384 extensiones 204 enlaces troncales 240 canales
Diagnostico del equipo		
Falla	causa	solución
Se observa polvo en el exterior, cableado con malas características estéticas y no se ha realizado respaldo de la configuración del equipo	uso cotidiano	Se realiza limpieza y reestructuración de cableado de conmutador y respaldo de configuración de extensiones telefónicas como parte de mantenimiento preventivo
Observaciones		
se recomienda cambiar enlaces de radio por uno de mejor capacidad para el servicio de telefonia emsad sin contratiempos		
Nombre y firma responsable del servicio		Nombre y Firma de conformidad del usuario
José Flores Lara		Informática

TLAXCALA COLEGIO DE ESTUDIOS CIENTÍFICOS Y TECNOLÓGICOS DEL ESTADO DIRECCION DE INFORMATICA

Av. Reforma No. 10, Col. Tlatempan, Apetatitlán, Tlaxcala, Tlax. Tel. 46 89200 (ext. 2016)
@cecytetlaxcala @TlaxcalaEMSaD www.cecytlax.edu.mx

TLAXCALA UNA NUEVA HISTORIA · EDUCACIÓN · SEPE · USET · CECYTE · EMSAD

COLEGIO DE ESTUDIOS CIENTÍFICOS Y TECNOLÓGICOS DEL ESTADO DE TLAXCALA
DIRECCIÓN DE INFORMÁTICA

REPORTE DE MANTENIMIENTO		
Fecha	Realizo	Área o plantel
17/01/22	José Flores Lara	Dirección de Informática
Descripción del equipo		
Equipo	Marca y Modelo	Datos Técnicos
Red de datos del colegio	N/A	Firewall Fortigate300E y red con 144 Nodos con switch cisco SF300
Diagnostico del equipo		
Falla	causa	solución
se solicita revisar acceso a carpetas compartidas y validar seguridad de sistemas de información instalados en la dirección	uso cotidiano	Se realiza análisis de red local, redes inalámbricas, acceso remoto a servidores de sistemas de información del colegio.
Observaciones		
Se analizo 18 equipos en la red local (192.168.0.0/23) que comparten archivos y se encuentran configurados con acceso por contraseña. No se encontró información compartida sin contraseña. Las redes inalámbricas se encuentran en vlan diferentes y no se permite el salto de la red local hacia ellas por definición en el equipo Fortigate300. Únicamente existe el salto entre la red de directores y DG a la red por cable para que los usuarios puedan imprimir. El acceso remoto a recursos del colegio en mediante el uso de VPN con validación de dos pasos. La configuración de proxy inverso oculta los servidores al exterior.		
Nombre y firma responsable del servicio		Nombre y Firma de conformidad del usuario
José Flores Lara		

TLAXCALA
Informática
COLEGIO DE ESTUDIOS CIENTÍFICOS Y TECNOLÓGICOS DEL ESTADO
DIRECCION DE INFORMÁTICA

Av. Reforma No. 10, Col. Tlatempan, Apetatitlán, Tlaxcala, Tlax. Tel. 46 89200 (ext. 2418/2016)
@cecytetlaxcala · @TlaxcalaEMSaD · www.cecytlax.edu.mx

TLAXCALA UNA NUEVA HISTORIA EDUCACIÓN SEPE USET CECYTE EMSAD

COLEGIO DE ESTUDIOS CIENTÍFICOS Y TECNOLÓGICOS DEL ESTADO DE TLAXCALA

DIRECCIÓN DE INFORMÁTICA

REPORTE DE MANTENIMIENTO		
Fecha	Realizo	Área o plantel
23/03/22	José Flores Lara	Dirección de Informática
Descripción del equipo		
Equipo	Marca y Modelo	Datos Técnicos
Servidor virtual de tickets	Dell powerEdge R440	1 CPU con 512MB de RAM y 8GB de almacenamiento
Diagnostico del equipo		
Falla	causa	solución
El servicio web de plataforma ticket se hace lenta	El Monitoreo de los recursos muestra saturación de memoria RAM y de memoria swap(memoria de intercambio).	Se asigna 1GB de memoria RAM y 1GB de memoria swap mediante consola de administración PROXMOX
Observaciones		
Monitoreo posterior a la asignación muestra desempeño del 40% de uso de recursos de memoria, un valor aceptable dentro del rango de uso. Se adjunta evidencia de cambio de memoria RAM		
Nombre y firma responsable del servicio		Nombre y Firma de conformidad del usuario
José Flores Lara		Informática

TLAXCALA

COLEGIO DE ESTUDIOS CIENTÍFICOS Y TECNOLÓGICOS DEL ESTADO DIRECCION DE INFORMÁTICA

Av. Reforma No. 10, Col. Tlatempan, Apetatitlan, Tlaxcala, Tlax. Tel. 46 89200 (ext. 2016)
@cecytetlaxcala @TlaxcalaEMSaD www.cecytlax.edu.mx