COLEGIO DE ESTUDIOS CIENTÍFICOS Y TECNOLÓGICOS DEL ESTADO DE HIDALGO.
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN (INFORMATICA).

MANUAL DE RECUPERACIÓN DE DESASTRES

Introducción

La infraestructura de tecnologías de la información, es parte vital dentro de toda organización, debido a que son los elementos transversales a todos los procesos operativos y funcionales. Dentro de los elementos que componen la infraestructura de Tecnologías de la Información, se pueden mencionar todos y cada uno de los dispositivos activos necesarios para la transmisión de la información, al igual que los distintos medios que permiten la interacción de la misma. La infraestructura de TI soporta todos los servicios y aplicaciones necesarias para el desarrollo de la organización, siendo este un punto crítico a salvaguardar.

La administración de riesgos es un proceso continuo que implica identificar, evaluar y mitigar los riesgos que enfrenta una organización. En el contexto de un área informática que se encarga de la gestión de servidores locales, los riesgos pueden incluir amenazas a la seguridad de la información, fallas en los sistemas, errores humanos, entre otros. Este manual tiene como objetivo proporcionar una guía básica para la identificación, evaluación y mitigación de estos riesgos.

Objetivo

El siguiente es un manual básico de administración de riesgos para un área informática que se encarga de la gestión de servidores locales, así como cada uno de los dispositivos activos necesarios para la transmisión de la información, y los distintos medios que permiten la interacción de la misma. Este manual se centra en la identificación, evaluación y mitigación de riesgos relacionados con la seguridad de la información y la continuidad del servicio en el contexto de los servidores locales.

Justificación

Actualmente los procesos de la Dirección General de CECyTE Hidalgo están siendo soportados por la tecnología, procesos alojados en servidores, sistemas informáticos, base de datos y activos para la transmisión de la información y su comunicación para su eficiente flujo. El sitio físicamente hablando donde están los equipos con características diferentes a una computadora de uso normal, es el bien llamado **site**, un lugar físico con ciertas características de voltaje, clima, y seguridad, de donde radica su importancia, debido a que se alojan los servidores, switch, conmutador y recepción de varios servicios de comunicaciones, el cual está expuesto a múltiples amenazas (inundaciones, <incendios, terremotos, apagones, errores humanos y/o intencionados, etc.) donde se afecte el funcionamiento y genere un impacto de manera catastrófico.

Motivo por el cual es necesario contar con un proceso para asegurar la alta disponibilidad de las tecnologías de la información con las que cuenta el Colegio, para ello, a través del plan de recuperación de desastres, donde se manifiesten tanto las buenas prácticas y estar preparado para la mala praxis, permita al Colegio la disponibilidad de los procesos que día a día son ejecutados por personal para el eficiente funcionamiento del Colegio. La importancia de contar con procedimientos contingentes para cuando se presente un evento catastrófico, permitirá que no se interrumpa la operatividad de los procedimientos y/o servidores del Colegio.

Identificación de riesgos

La identificación de riesgos es el primer paso en la administración de riesgos. Para identificar los riesgos asociados con la gestión de servidores locales, se recomienda lo siguiente:
Realizar una evaluación de riesgos inicial: Esta evaluación puede incluir una revisión de la documentación existente, como los acuerdos de nivel de servicio (SLA), las políticas y los procedimientos de seguridad. También puede incluir entrevistas con el personal de TI y otros stakeholders relevantes para identificar los riesgos potenciales.
Identificar las amenazas a la seguridad de la información: Las amenazas pueden incluir ataques cibernéticos, malware, phishing, ingeniería social, entre otros.
Identificar las vulnerabilidades del sistema: Las vulnerabilidades pueden incluir sistemas operativos y aplicaciones desactualizados, contraseñas débiles, permisos excesivos, entre otros.
Identificar los riesgos asociados con el personal: Estos riesgos pueden incluir errores humanos, mala gestión de contraseñas, entre otros.
Identificar los riesgos asociados con los procesos: Estos riesgos pueden incluir la falta de documentación, la falta de pruebas adecuadas, entre otros.

TABLAS EVALUACIÓN DE RIESGOS

Definición		Descripción
C	Confidencialidad	¿Qué nivel de riesgo representaría para la organización que el activo fuera conocido por personas no autorizadas?
I	Integridad	¿Qué nivel de riesgo representaría para la organización que los activos fueran modificados fuera de control?
D	Disponibilidad	¿Qué nivel de riesgo representaría para la organización que el activo no estuviera disponible?
A	Autenticidad	¿Qué nivel de riesgo representaría para la organización que quien accede al servicio no sea realmente quien se cree?
T	Trazabilidad	¿Qué nivel de riesgo representaría para la organización que no quedara constancia del uso del servicio o el acceso al mismo?

Evaluación de riesgos
Se podrán aplicar las técnicas de gestión de riesgos de la norma EC0536 a todos los sistemas informáticos.

El proceso de evaluación de riesgos debe considerar:

a) La importancia de la información, del software y de otros activos del sistema informático en cuestión;
b) Las actividades de la Dirección General de CECyTEH, los productos y servicios respaldados por los sistemas informáticos en cuestión;
c) El daño que pueda causarse como consecuencia de una violación seria de la seguridad de la información. Los impactos potenciales incluyen la pérdida financiera, académica
d) La probabilidad real de que ocurra dicha violación, teniendo en cuenta los controles existentes y las amenazas imperantes, el entorno en el que se utiliza o funciona el sistema, y la vida útil real de la información en cuestión;
e) Los controles adicionales requeridos para reducir los riesgos a un nivel aceptable;
f) Si la Dirección de Informática de CECyTEH considera que los riesgos identificados por esta evaluación son inaceptables, y estos no se pueden evitar ni reducir satisfactoriamente a través de métodos más efectivos, entonces se deben planificar e implementar mejoras en la seguridad informática.

Una vez que se han identificado los riesgos, se debe evaluar su probabilidad e impacto. La evaluación de riesgos implica responder las siguientes preguntas:
¿Cuál es la probabilidad de que el riesgo ocurra?
¿Cuál sería el impacto si el riesgo se materializara?
Para evaluar la probabilidad, se puede utilizar una escala de 1 a 5, donde 1 significa que el riesgo es poco probable y 5 significa que el riesgo es muy probable. Para evaluar el impacto, se puede utilizar una escala de 1 a 5, donde 1 significa que el impacto es bajo y 5 significa que el impacto es muy alto.

Valor	Nivel
1	Riesgo muy bajo
2	Riesgo bajo
3	Riesgo medio
4	Riesgo alto
5	Riesgo muy alto

Mitigación de riesgos

La mitigación de riesgos implica implementar controles para reducir la probabilidad o el impacto de los riesgos identificados. Algunas medidas de mitigación que se pueden implementar incluyen:
Implementar medidas de seguridad de la información, como cortafuegos, antivirus y detección de intrusiones.

Actualizar regularmente los sistemas operativos y aplicaciones para mitigar las vulnerabilidades del sistema. Implementar políticas y procedimientos para la gestión de contraseñas y la asignación de permisos.
Proporcionar capacitación regular al personal para mejorar

CRONOGRAMA DE ACTIVIDADES

No.	Actividades	Semana 1	Semana 2	Semana 3	Semana 4
1	Planificar las distintas actividades que permitan realizar el proceso de análisis de riesgos.				
2	Revisar información relacionada con el área de TI, identificando los activos, las amenazas a que estos están expuestos y las respectivas responsivas.				
3	Analizar y valorar los riesgos.				
4	Elaborar el instrumento de recolección de la información.				
5	Desarrollar la auditoría apoyada en una herramienta de recolección de datos.				
6	Aplicar el instrumento de recolección de la información.				
7	Analizar la información recopilada en la actividad anterior.				
9	Elaborar un informe con los resultados obtenidos.				
10	Comunicar a los miembros de la alta Dirección el informe elaborado.				
11	Presentar mejoras al área de Transformación Tecnológica en cuanto a la seguridad de los activos teniendo en cuenta los hallazgos obtenidos.				

Responsabilidades:
La dirección de informática que pertenece al Cecyte Hidalgo es la responsable de mantener la alta disponibilidad de los procesos, así como el contar con un plan en caso de desastres, haciéndolo a través de:

Preparación para casos de emergencias
Consiste en saber que es necesario para que los procesos sigan en funcionamiento en caso de una contingencia

- Energía eléctrica (doble subministro o a través de baterías)
- Servidores Doble fuente de poder (energía independiente), doble de todo
- Información (respaldos mediante bitácoras, diaria, semanal, mensual y anual)
- Switch´s redundancia física y lógica
- Comunicaciones redundancia ya sea con el mismo proveedor, pero diferente ruta y/o con otro proveedor.

Respuesta a una emergencia
Es la identificación de la contingencia y la acción que se tiene que ejecutar para regresar a la normalidad los servicios y procesos a los usuarios, siendo este regreso a la normalidad en el menor tiempo posible manteniendo en óptimas condiciones la información, infraestructura, todo con base a los procesos y rutas de recuperación para volver a la normalidad.
Ya resuelta la contingencia, se debe realizar un análisis detallado de lo sucedido para identificar las causas raíz del problema y determinar las medidas preventivas necesarias para evitar futuras contingencias similares.

Pruebas y simulacros
Son de vital importancia ya que es el entrenamiento en el cual simulamos la ausencia de algún elemento importante que interrumpa la disponibilidad de los procesos y la acción o proceso de recuperación que se aplicara en caso de la ausencia de algún daño. También nos sirve para una adecuada identificación o carencia en donde tengamos algún problema el cual se tenga que corregir y/o donde tengamos que hacer una inversión económica para la compra de algún equipo que sea necesario o la inversión de un servicio adicional.

Creación de:

- Bitácoras de ingreso al site, con la finalidad de contar con un mejor control
- Habilitar una video cámara y grabación, para que nos sirva de monitoreo de lo que acontece en el SITE.
- Bitácoras de respaldo de información, aquí es donde entra el **Que** se va a respaldar (sistema, programa, base de datos) **Como** se va a desarrollar las actividades, **Donde** se va a respaldar, medio en el cual se realizaran los respaldos ya sean DVD, discos duros, la nube, **Cuando** periodicidad y frecuencia de los respaldos conforme a lo que se va a respaldar.

Identificación de puntos vulnerables

- Saber dónde tenemos áreas de oportunidad de mejora tanto física como lógica, teniendo como finalidad la alta disponibilidad de los procesos del colegio.
- Realizar una evaluación de riesgos de seguridad informática periódica para identificar posibles amenazas y vulnerabilidades en el sistema de información y en la infraestructura tecnológica.
- Establecer políticas y procedimientos de seguridad informática para proteger los activos de información y la infraestructura tecnológica de posibles riesgos y amenazas.
- Implementar medidas de seguridad física, como cámaras de vigilancia, control de acceso y sistemas de detección y extinción de incendios, para proteger la infraestructura tecnológica de daños y amenazas.
- Realizar pruebas y simulacros para evaluar la eficacia del plan de contingencia y recuperación ante situaciones de emergencia o desastres.
- Mantener actualizado el plan de contingencia y recuperación, así como los respaldos de la información crítica, para asegurar la rápida recuperación de los procesos y servicios en caso de una contingencia.
- Realizar capacitaciones y entrenamientos al personal para que estén preparados ante situaciones de emergencia y conozcan los procedimientos y acciones a seguir para garantizar la continuidad de los procesos y servicios.

TÉCNICAS DE RECOLECCIÓN

Los instrumentos para recopilar la información son los siguientes:

- Vistas y recolección de inventario en sitio que permitan verificar, evaluar la existencia y ubicación de los activos TI.
- Tablero de control de activo
- Checklist de comportamiento de la red en sitio.
- Actualización de cartas responsivas.
- Cumplimiento del cronograma de mantenimiento correctivo.

DESARROLLO DE ACTIVIDADES

CLASIFICACIÓN DE ACTIVOS TI

Tipo	Activo
Equipamiento de Cómputo	Impresora
	PC o computadora de escritorio
	Portátil (Laptop o Macbook)
	TV
	Proyector
	Monitor
	Mouse
	Teclado
Redes de comunicaciones	Router
	Modem
	Punto de Acceso
	Red cableada
	Red inalámbrica
	Móviles
Equipamiento auxiliar	No break
Recurso Humano	Personal de TI

HERRAMIENTAS DE EVALUACIÓN Y RECOLECCIÓN

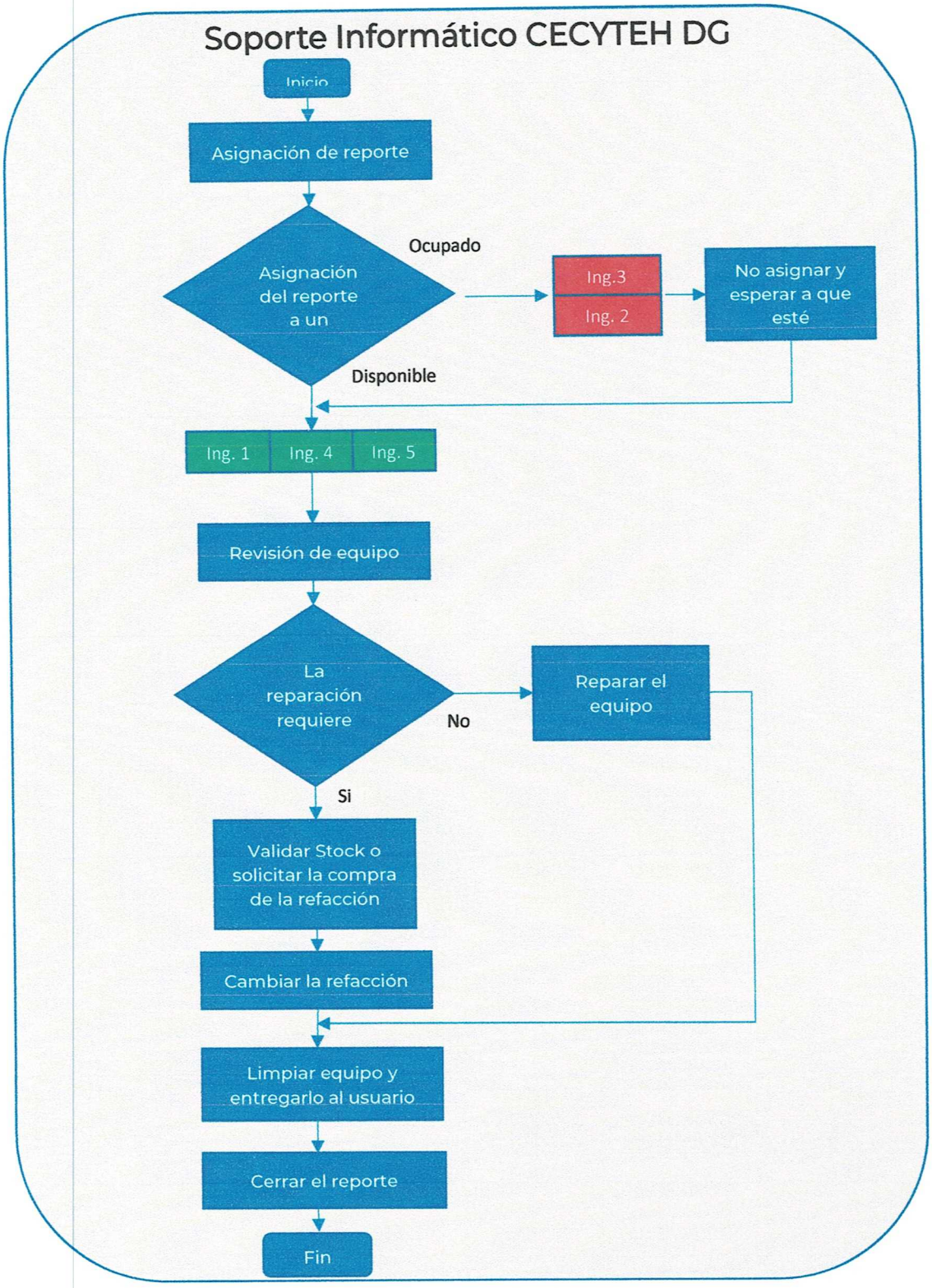
Nombre	Documento
Control de activo TI	Informe
Cronograma de mantenimiento preventivo	Cronograma de mantenimiento preventivo
Recepción de equipo y pruebas de funcionalidad	Recepción de equipo y pruebas de funcionalidad
Checklist de identificación de amenazas y vulnerabilidades	Checklist de identificación de amenazas y vulnerabilidades
Herramienta de evaluación con base a la norma ISO/IEC 27002:2013	Herramienta de evaluación en base a la norma ISO/IEC 27002:2013

ORDEN DE ACTIVIDADES

El orden de actividades se pretende realizar por cada día de visita a las sucursales y patios como se describe a continuación:

1. Checklist de amenazas y vulnerabilidades en sitio.
2. Checklist de evaluación en base a la norma ISO 27000.
3. Recolección de inventario de activos TI.
4. Mantenimiento preventivo.
5. Recepción de equipo y pruebas de funcionalidad.
6. Capacitación a personal.

DIAGRAMAS DE PROCESOS



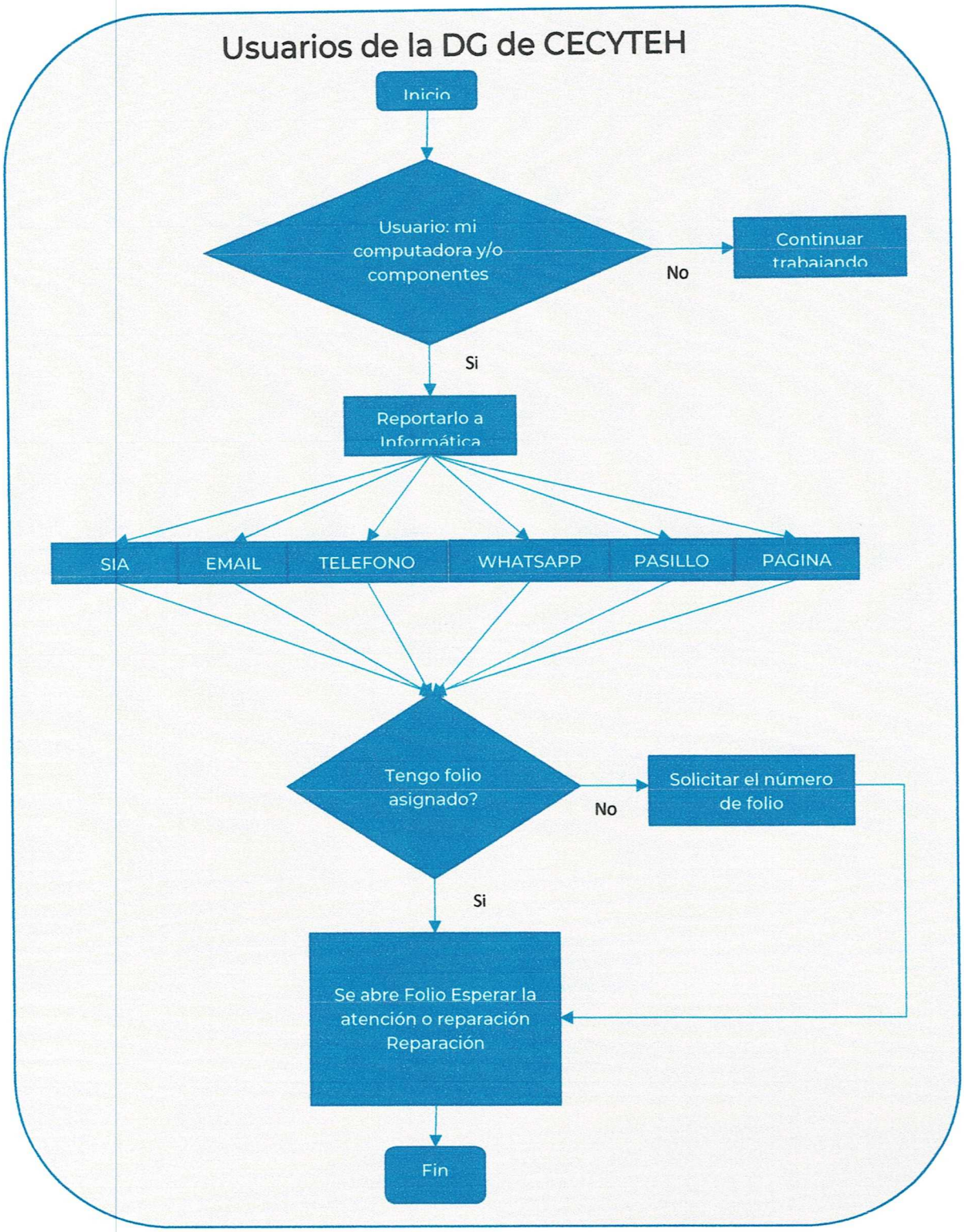
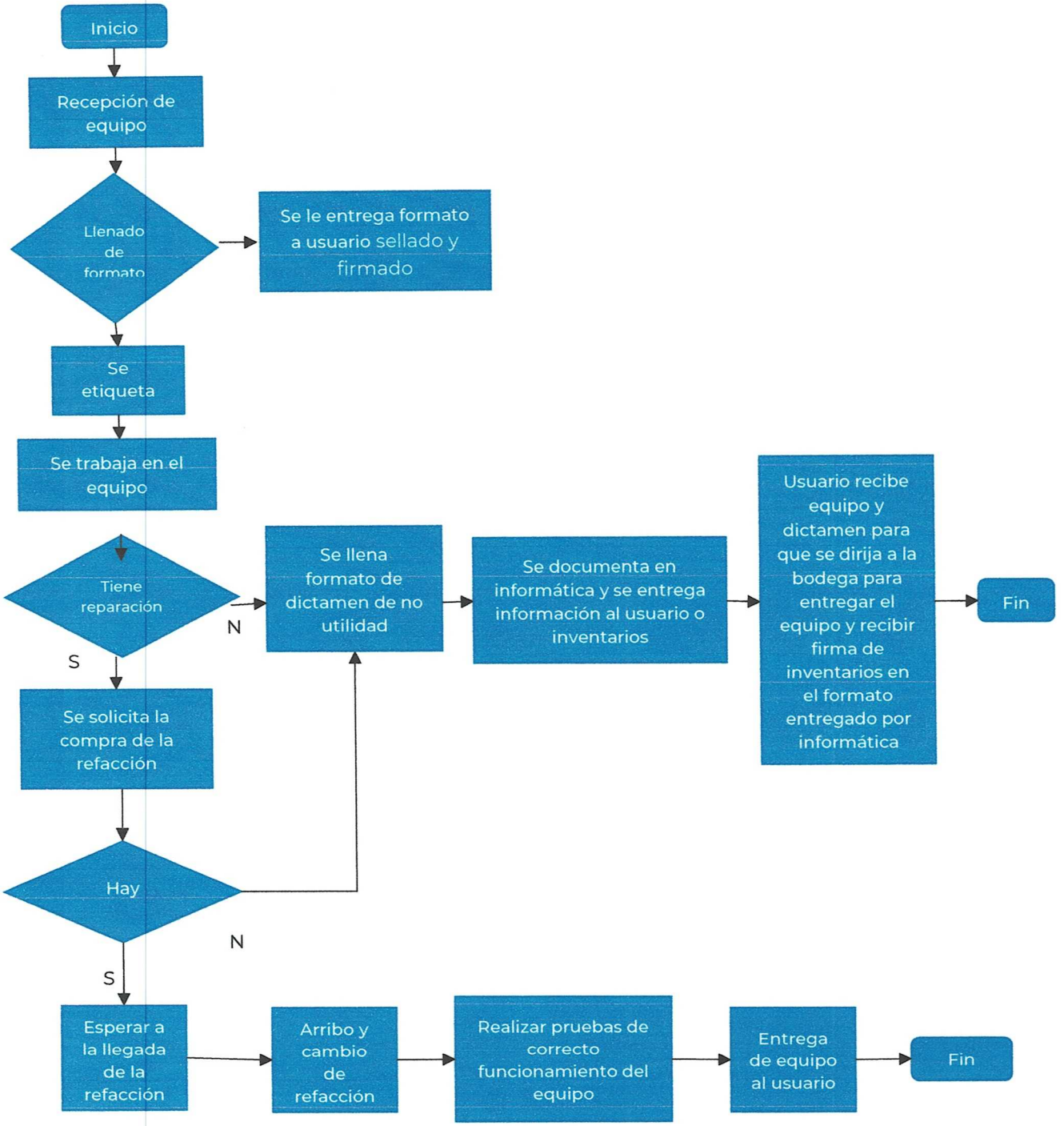

Usuarios de la DG de CECYTEH
Inicio
Usuario: mi computadora y/o componentes
No
Continuar trabajando
Si
Reportarlo a Informática
SIA
EMAIL
TELEFONO
WHATSAPP
PASILLO
PAGINA
Tengo folio asignado?
No
Solicitar el número de folio
Si
Se abre Folio Esperar la atención o reparación Reparación
Fin

Diagrama de flujo para la atención de equipo de computo



Dirección: Circuito Ex Hacienda La Concepción. Lote 17. Edificio B, San Juan Tilcuautla, C.P. 42160, Municipio de San Agustín Tlaxiaca, Hidalgo, México,
Teléfono: 01 (771) 717 07 30 ext. 1052
http://www.cecyteh.edu.mx

MARCO TEÓRICO

Activos: Recursos que forman parte de la organización como hardware, software, datos, infraestructura.

Amenaza: Posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la seguridad de la información, los elementos de Información.

Ciclo PDCA: También conocido como Ciclo PHVA viene de las siglas Planificar, Hacer, Verificar y Actuar, en inglés "Plan, Do, Check, Act". Esta metodología describe los cuatro pasos esenciales que se deben llevar a cabo de forma sistemática para lograr la mejora continua, entendiendo como tal al mejoramiento continuado de la calidad (disminución de fallos, aumento de la eficacia y eficiencia, solución de problemas, previsión y eliminación de riesgos potenciales.).

Confidencialidad: es una de las propiedades de los activos de información que garantiza que solo personas autorizadas pueden acceder a esta.

Datos: Son todos aquellos conceptos, cifras, instrucciones que se tienen aisladas entre sí, sin seguir una organización o un orden específico.

Disponibilidad: característica de los activos que implica el acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados en el momento que lo requieran.

Hardware: parte tangible de un equipo de cómputo o dispositivo tecnológico, es decir, todos sus componentes físicos.

Información: conjunto de datos, añadidos, procesados y relacionados, de manera que pueden dar pauta a la correcta toma de decisiones según el fin previsto.

Integridad: cualidad de los activos de información donde se asegura que la información y sus métodos de proceso se mantengan exactos y completos.

Mantenimiento Correctivo: proceso mediante el cual se realizan las correcciones de las averías o fallas, de un equipo de cómputo, cuando éstas se presentan.

Mantenimiento Preventivo: es el conjunto de actividades que se desarrollan con el objeto de proteger los equipos de posibles fallas, utilizando métodos de limpieza física y también métodos basados en el uso de software.

Política de Seguridad: consiste en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan.

Seguridad de la información: es todo el conjunto de técnicas y acciones que se implementan para controlar y mantener la privacidad de la información y datos de una institución; y asegurarnos que esa información no salga del sistema de la empresa y caigan en las manos equivocadas.

Integridad: cualidad de los activos de información donde se asegura que la información y sus métodos de proceso se mantengan exactos y completos.

Mantenimiento Correctivo: proceso mediante el cual se realizan las correcciones de las averías o fallas, de un equipo de cómputo, cuando éstas se presentan.

Mantenimiento Preventivo: es el conjunto de actividades que se desarrollan con el objeto de proteger los equipos de posibles fallas, utilizando métodos de limpieza física y también métodos basados en el uso de software.

Política de Seguridad: consiste en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan.

Seguridad de la información: es todo el conjunto de técnicas y acciones que se implementan para controlar y mantener la privacidad de la información y datos de una institución; y asegurarnos que esa información no salga del sistema de la empresa y caigan en las manos equivocadas.

Sistema de Gestión de Seguridad de la Información: proporciona un modelo para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la protección de los activos de información para alcanzar los objetivos de negocio.

Software: son todos los programas informáticos que hacen posible la realización de tareas específicas dentro de un computador.

Trazabilidad: propiedad de los activos de información que permite asegurar que en todo momento se podrá determinar quién realizó cierta actividad y en qué momento lo hizo.

Vulnerabilidad: es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacidad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

	Elaboró:	Autorizó:
Puesto	**Director de Informática**	**Director General**
Fecha		
Nombre y firma	**Aldo Serafín Pedraza Montiel**	**Agustín Rowe Córdova**