<h1>Del fallo a la solución: diseño de un plan de contingencia para reparar equipos de cómputo</h1>

Ciencias de la Educación | Licenciatura en tecnología e informática | Aprendizaje Basado en Proyectos

Descripción

Este plan de clase está dirigido a estudiantes de la Licenciatura en Tecnología e Informática y aborda los componentes clave de un plan de contingencia aplicado a la reparación y recuperación de equipos de cómputo. Durante dos sesiones de 120 minutos, los estudiantes trabajarán mediante la metodología de Aprendizaje Basado en Proyectos para responder a una situación realista: un laboratorio de informática presenta fallas simultáneas en varios equipos y necesita mantener la continuidad del servicio, proteger la información y organizar una respuesta técnica segura.

Los estudiantes analizarán riesgos frecuentes, establecerán prioridades de atención, definirán procedimientos de respaldo y recuperación, asignarán responsabilidades, identificarán recursos necesarios y elaborarán un plan de contingencia técnico. El producto final será un documento aplicable a un laboratorio, aula de informática o pequeño centro de soporte, acompañado de una simulación de respuesta ante una falla.

La propuesta favorece el trabajo colaborativo, la toma de decisiones, la comunicación técnica y la autonomía. Asimismo, conecta los contenidos con situaciones que pueden presentarse en prácticas profesionales, servicios de mantenimiento, soporte a usuarios, emprendimientos tecnológicos y administración de laboratorios. El plan no se limita a reparar un equipo, sino que promueve anticipar problemas, reducir tiempos de inactividad, proteger los datos y garantizar que las operaciones puedan continuar de manera organizada y segura.

Objetivos de Aprendizaje

- **Identificar** los componentes esenciales de un plan de contingencia aplicado a la reparación y recuperación de equipos de cómputo.
- **Analizar** riesgos, fallas y consecuencias operativas para establecer prioridades de atención técnica.
- **Diseñar** colaborativamente un plan de contingencia que incluya prevención, respuesta, recuperación, responsables, recursos y comunicación.
- **Aplicar** procedimientos básicos de respaldo, diagnóstico inicial, escalamiento y recuperación ante una situación simulada.
- **Evaluar** la pertinencia, claridad, viabilidad y seguridad del plan elaborado por el equipo.

Recursos Necesarios

- Computadores o portátiles: uno por cada grupo de tres o cuatro estudiantes.
- Proyector, pantalla y acceso a internet.

- Presentación digital del docente sobre planes de contingencia y continuidad operativa.
- Video breve de 3 a 5 minutos sobre una falla crítica en un laboratorio de informática.
- Guías impresas con casos de fallas: daño eléctrico, infección por malware, pérdida de datos, sobrecalentamiento, falla de disco y caída de red.
- Formato impreso o digital para elaborar el plan de contingencia.
- Lista de cotejo y rúbrica de evaluación.
- Hojas tamaño carta, cartulina o papelógrafo, marcadores y notas adhesivas.
- Diagrama de flujo editable en Canva, diagrams.net o Microsoft Visio.
- Documento colaborativo en Google Docs o Microsoft 365.
- Hoja de cálculo en Google Sheets o Microsoft Excel para matriz de riesgos y priorización.
- Herramientas de diagnóstico disponibles en el sistema operativo, como Administrador de tareas, Visor de eventos, Diagnóstico de memoria y herramientas de almacenamiento.
- Dispositivo externo o carpeta simulada para representar copias de seguridad. No se deben manipular datos reales sin autorización.
- Tarjetas de roles: coordinador, técnico de diagnóstico, responsable de respaldo y responsable de comunicación.

Requisitos Previos

- Reconocer los componentes básicos de un computador y sus funciones principales.
- Aplicar normas básicas de seguridad eléctrica, seguridad física y protección de componentes.
- Comprender las etapas generales de diagnóstico y mantenimiento preventivo y correctivo.
- Utilizar herramientas básicas del sistema operativo para consultar información del equipo.
- Interpretar conceptos como copia de seguridad, sistema operativo, red, malware, almacenamiento y usuario.
- Trabajar colaborativamente, registrar procedimientos técnicos y comunicar hallazgos de manera clara.
- Relacionar el contenido con aprendizajes previos sobre mantenimiento de hardware, software y soporte técnico.

Actividades

Sesión 1: Reconocer riesgos y estructurar el plan de contingencia

Fase de Inicio

Tiempo estimado: 15 minutos

Propósito de la sesión

En esta primera sesión, los estudiantes comprenderán por qué un técnico no debe limitarse a reparar el equipo que ya falló. Analizarán cómo una contingencia puede afectar la información, la continuidad de las clases, la atención a

usuarios y la seguridad de los dispositivos. El propósito es iniciar el proyecto de diseño de un plan de contingencia para un laboratorio de informática.

Activación de conocimientos previos

Docente: Proyecta la pregunta: “Son las 7:30 a. m. y diez computadores de un laboratorio no encienden. Hay una clase programada en 30 minutos. ¿Qué harían primero, qué no harían y qué información necesitarían antes de intervenir?”. Solicita que cada estudiante escriba durante dos minutos tres acciones iniciales y un riesgo de actuar apresuradamente.

Estudiantes: Responden individualmente, comparan sus respuestas con un compañero y comparten una decisión en plenaria. El docente registra en el tablero las palabras diagnóstico, prioridad, respaldo, seguridad, comunicación y recuperación.

Motivación y enganche

Docente: Presenta un video breve o una imagen secuencial de un laboratorio afectado por una falla eléctrica y pregunta: “¿El problema consiste únicamente en que los computadores no encienden?”. Después plantea el reto: “En dos sesiones, su equipo será contratado como grupo de soporte para diseñar un plan que permita responder a la contingencia y reanudar el servicio con el menor impacto posible”.

Estudiantes: Identifican consecuencias técnicas y administrativas: pérdida de información, interrupción de clases, usuarios afectados, equipos fuera de servicio y necesidad de informar a responsables.

Contextualización

Docente: Relaciona el reto con escenarios profesionales: un aula de informática, una sala de soporte, un cibercafé o un emprendimiento de reparación. Explica que un plan de contingencia organiza las acciones antes, durante y después de una falla, y que debe ser claro para que otra persona pueda ejecutarlo.

Estudiantes: Seleccionan un contexto para su proyecto y mencionan una experiencia cotidiana en la que una falla tecnológica haya interrumpido una actividad. El docente comunica el producto final, los criterios de evaluación y la organización de los equipos.

Fase de Desarrollo

Tiempo estimado: 95 minutos

Presentación del contenido mediante el proyecto

Tiempo estimado: 20 minutos. El docente presenta el reto del proyecto: “Diseñar un plan de contingencia para un laboratorio con 20 computadores, un servidor de archivos, conexión a internet, impresora de red y usuarios que necesitan continuar trabajando”. En lugar de realizar una exposición extensa, entrega a cada grupo una ficha con información parcial del laboratorio.

- **Docente:** Explica los componentes que deben aparecer en todo plan: identificación del riesgo, alcance, objetivos, criterios de activación, inventario de equipos y recursos, roles y responsables, procedimientos de prevención,

respuesta y recuperación, respaldo de información, comunicación, escalamiento, documentación y revisión.

- **Docente:** Presenta el ciclo “prevenir, responder, recuperar y mejorar” y ejemplifica con una falla de disco: prevención mediante copias de seguridad; respuesta mediante aislamiento del equipo; recuperación mediante sustitución del disco y restauración; mejora mediante revisión del procedimiento.
- **Estudiantes:** Elaboran un esquema inicial en sus cuadernos y formulan una pregunta técnica que necesiten resolver para diseñar el plan.

Actividad 1: Detectives de riesgos tecnológicos

Tiempo estimado: 30 minutos. Objetivo específico: Identificar y analizar riesgos, fallas y consecuencias operativas.

Organización: Grupos de tres o cuatro estudiantes.

- **Docente:** Entrega a cada grupo un caso diferente: sobretensión eléctrica, ransomware, falla de disco, sobrecalentamiento, pérdida de conectividad o error de actualización.
- **Docente:** Indica: “Lean el caso y completen la matriz con las columnas: riesgo, causa probable, equipos o datos afectados, impacto, probabilidad, señales de alerta y primera acción segura”.
- **Estudiantes:** Subrayan en el caso la información relevante, diferencian causa y consecuencia y asignan una valoración de impacto y probabilidad en escala de 1 a 3.
- **Estudiantes:** Priorizan dos riesgos utilizando la fórmula cualitativa “prioridad = impacto x probabilidad” y justifican cuál debe atenderse primero.
- **Docente:** Recorre los grupos y pregunta: “¿Qué evidencia tienen para considerar que el impacto es alto?”, “¿Qué acción podría agravar el daño?” y “¿Qué información falta antes de intervenir?”.
- **Producto:** Matriz de riesgos con al menos cuatro riesgos identificados y dos riesgos priorizados.

Actividad 2: Rompecabezas de los componentes del plan

Tiempo estimado: 30 minutos. Objetivo específico: Identificar la función de cada componente de un plan de contingencia.

Organización: Grupos de cuatro estudiantes con roles rotativos.

- **Docente:** Entrega tarjetas con nombres de componentes y tarjetas con descripciones mezcladas. Por ejemplo: “criterio de activación”, “responsable técnico”, “procedimiento de recuperación”, “canal de comunicación” e “inventario de recursos”.
- **Estudiantes:** Relacionan cada componente con su descripción y con una acción concreta para el caso asignado.
- **Estudiantes:** Ordenan los componentes en una secuencia de uso: preparación, detección, activación, respuesta, recuperación y revisión.
- **Docente:** Solicita que cada grupo explique dos relaciones. Pregunta: “¿Qué diferencia existe entre responder y recuperar?”, “¿Quién decide activar el plan?” y “¿Cómo se registra lo realizado?”.

- **Estudiantes:** Corrigen el orden si reciben observaciones y elaboran un organizador gráfico en papel o en diagrams.net.
- **Producto:** Organizador gráfico de los componentes del plan y explicación oral de su función.

Actividad 3: Primer borrador del plan

Tiempo estimado: 15 minutos. Objetivos específicos: Diseñar la estructura inicial de un plan y establecer responsabilidades.

- **Docente:** Entrega el formato del proyecto con los apartados: contexto, objetivo, alcance, riesgos prioritarios, criterios de activación, responsables y recursos.
- **Estudiantes:** Seleccionan los riesgos principales de su matriz y redactan el objetivo de su plan usando la fórmula: “Garantizar la continuidad de _____ ante _____ mediante _____”.
- **Estudiantes:** Distribuyen roles: coordinador de contingencia, técnico de diagnóstico, responsable de respaldo y responsable de comunicación.
- **Docente:** Revisa que los roles no sean solo nombres y pregunta: “¿Qué decisión puede tomar cada responsable?”, “¿A quién informa?” y “¿Qué evidencia debe dejar?”.
- **Producto:** Primer borrador con objetivo, alcance, riesgos y responsables.

Diferenciación y transiciones

Para quienes necesiten apoyo, el docente ofrece una matriz parcialmente completada, un glosario visual y un ejemplo de riesgo resuelto. También permite explicar oralmente una decisión antes de redactarla. Para quienes terminan antes, se propone agregar un riesgo relacionado con proveedores externos, estimar tiempos máximos de recuperación y proponer un indicador de éxito. La transición se realiza diciendo: “Ya sabemos qué puede fallar y quién participa; ahora debemos cerrar el borrador y comprobar si las decisiones son claras”.

Fase de Cierre

Tiempo estimado: 10 minutos

Síntesis

Docente: Solicita que cada grupo complete en una nota adhesiva la frase: “Un plan de contingencia no es solo una lista de reparaciones; también incluye _____, _____ y _____”. Los grupos colocan sus respuestas en un mural organizado en las categorías prevención, respuesta y recuperación.

Estudiantes: Comparan las respuestas y corrigen una idea inicial que haya cambiado durante la sesión.

Reflexión metacognitiva

- ¿Qué riesgo priorizamos y qué evidencia utilizamos para justificarlo?
- ¿Qué componente del plan nos resultó más difícil de definir y por qué?
- ¿Qué acción insegura podría empeorar la falla del caso analizado?

Retroalimentación y transferencia

Docente: Proporciona retroalimentación inmediata usando dos fortalezas y una pregunta de mejora por grupo. Verifica que todos los borradores incluyan un objetivo, riesgos y responsables. Anticipa que en la siguiente sesión los estudiantes convertirán el borrador en procedimientos concretos y lo probarán mediante una simulación.

Tarea o reto: Cada estudiante debe observar en casa o en una institución cercana un posible riesgo tecnológico y registrar: riesgo, consecuencia, medida preventiva y responsable de atenderlo. No debe intervenir equipos ni recopilar información privada.

Sesión 2: Diseñar, probar y mejorar el plan de contingencia

Fase de Inicio

Tiempo estimado: 10 minutos

Propósito de la sesión

La segunda sesión retoma los riesgos, componentes y borradores elaborados anteriormente para transformarlos en un plan operativo. Los estudiantes definirán procedimientos paso a paso, establecerán medios de comunicación y comprobarán la utilidad del documento mediante una simulación técnica.

Conexión con la sesión anterior

Docente: Solicita a cada grupo mencionar en 30 segundos el riesgo prioritario de su proyecto y el componente que todavía necesita desarrollar. Luego presenta tres preguntas de repaso: “¿Cuándo se activa un plan?”, “¿Qué se debe proteger primero?” y “¿Qué diferencia hay entre recuperación y mejora?”.

Estudiantes: Responden con tarjetas de colores: verde para una respuesta segura, amarillo para una respuesta incompleta y rojo para una respuesta que podría generar un riesgo. El docente aclara dudas y explica el producto final de la sesión.

Fase de Desarrollo

Tiempo estimado: 95 minutos

Revisión guiada del contenido

Tiempo estimado: 15 minutos. El docente muestra un ejemplo breve de procedimiento para una falla de disco: detectar síntomas, registrar el equipo, desconectarlo de la red si existe riesgo, verificar la disponibilidad de respaldo, escalar si se requiere autorización, reemplazar el componente, restaurar la información, probar el equipo y documentar el resultado. Destaca que un procedimiento debe indicar acción, responsable, recurso, tiempo aproximado y criterio para avanzar.

- **Docente:** Pregunta: “¿Qué paso protege la información?”, “¿Qué paso evita ampliar el daño?” y “¿Qué evidencia confirma que el equipo fue recuperado?”.
- **Estudiantes:** Comparan el ejemplo con su borrador y marcan los apartados que deben completar.

Actividad 4: Construcción del procedimiento operativo

Tiempo estimado: 35 minutos. Objetivos específicos: Diseñar procedimientos de prevención, respuesta y recuperación; establecer roles, recursos y comunicación.

Organización: Los mismos grupos de proyecto.

- **Docente:** Indica: “Elaboren un procedimiento para el riesgo prioritario y otro para un riesgo secundario. Cada procedimiento debe tener: condición de activación, acciones numeradas, responsable, recursos, tiempo estimado, comunicación, criterio de escalamiento y evidencia de cierre”.
- **Estudiantes:** Redactan las medidas preventivas, como revisión de cables, control de temperatura, actualizaciones autorizadas y copias de seguridad verificadas.
- **Estudiantes:** Escriben las acciones de respuesta en verbos observables: aislar, registrar, verificar, notificar, diagnosticar, respaldar, reemplazar, restaurar y probar.
- **Estudiantes:** Definen la recuperación y la mejora: restauración de datos, validación con el usuario, actualización del inventario y reunión breve para revisar el incidente.
- **Docente:** Pregunta: “¿Qué debe hacerse antes de abrir el equipo?”, “¿Qué ocurre si no existe una copia de seguridad válida?”, “¿En qué momento se solicita apoyo externo?” y “¿Cómo se informa a los usuarios sin generar confusión?”.
- **Producto:** Dos procedimientos operativos integrados al documento del plan.

Actividad 5: Simulación de contingencia “Cinco minutos para decidir”

Tiempo estimado: 30 minutos. Objetivos específicos: Aplicar procedimientos de diagnóstico inicial, comunicación, escalamiento y recuperación; evaluar la viabilidad del plan.

Organización: Grupos de cuatro estudiantes. Cada grupo recibe una tarjeta de incidente distinta.

- **Docente:** Entrega el incidente sin anunciarlo previamente: “El servidor no permite acceder a los archivos”, “tres computadores muestran mensajes de cifrado”, “un equipo se apaga por temperatura”, “la red funciona intermitentemente” o “un equipo no reconoce su unidad de almacenamiento”.
- **Estudiantes:** Disponen de cinco minutos para activar el plan, asignar roles, indicar la primera acción segura y definir qué información deben registrar.
- **Estudiantes:** Representan durante diez minutos la respuesta: diagnóstico inicial, aislamiento o protección, consulta de respaldos, comunicación y decisión de escalar.
- **Docente:** Introduce una condición adicional, como “el respaldo más reciente tiene 24 horas” o “el usuario necesita el equipo en 20 minutos”. Los estudiantes ajustan la decisión sin omitir los controles de seguridad.
- **Observadores:** Si hay tiempo, otro grupo utiliza una lista de cotejo para verificar si se identificó el riesgo, se protegió la información, se comunicó el incidente y se documentó la acción.
- **Producto:** Registro de incidente, diagrama de decisiones y desempeño simulado.

Actividad 6: Revisión entre pares y versión final

Tiempo estimado: 15 minutos. Objetivo específico: Evaluar y mejorar la claridad, viabilidad y seguridad del plan.

- **Docente:** Entrega una lista de cotejo con cinco preguntas: “¿El riesgo está claramente descrito?”, “¿Las acciones están ordenadas?”, “¿Cada acción tiene responsable?”, “¿Se protege la información?” y “¿Se indica cuándo escalar?”.
- **Estudiantes:** Intercambian el documento con otro grupo, leen solo los apartados operativos y escriben una fortaleza y dos recomendaciones concretas.
- **Estudiantes:** Devuelven el documento, analizan las recomendaciones y realizan ajustes en la versión final.
- **Docente:** Verifica que las recomendaciones no impliquen acciones inseguras, como formatear sin respaldo, desconectar servidores sin autorización o instalar software no validado.
- **Producto:** Plan de contingencia final y registro de mejoras realizadas.

Diferenciación y transiciones

Para quienes necesiten apoyo, el docente proporciona una plantilla con frases iniciales: “Cuando ocurra…”, “El responsable de…”, “Antes de intervenir…”, “Se informará a…” y “El plan se considerará cerrado cuando…”. También puede permitir el uso de audio para explicar el procedimiento antes de transcribirlo. Para quienes terminan antes, se solicita incorporar un plan alterno cuando no exista respaldo, calcular el tiempo objetivo de recuperación y diseñar un indicador mensual de revisión. La transición hacia la simulación se realiza indicando: “Un plan solo es útil si puede ejecutarse; ahora comprobaremos qué tan claro resulta bajo presión”.

Fase de Cierre

Tiempo estimado: 15 minutos

Síntesis del aprendizaje

Docente: Solicita a cada grupo presentar en dos minutos su riesgo prioritario, la primera acción segura, el responsable principal y el criterio que confirma la recuperación. Mientras escuchan, los demás estudiantes completan un cuadro con tres columnas: “acción que previene”, “acción que responde” y “acción que recupera”.

Estudiantes: Presentan su solución, escuchan las preguntas de sus compañeros y entregan el plan final junto con la matriz de riesgos, el procedimiento y el registro de simulación.

Reflexión metacognitiva

- ¿Qué componente de nuestro plan permitió tomar decisiones con mayor rapidez?
- ¿Cómo comprobamos que la recuperación no solo encendía el equipo, sino que también protegía la información y permitía continuar el trabajo?
- Si aplicáramos este plan en un laboratorio real, ¿qué paso modificaríamos primero y por qué?

Retroalimentación

Docente: Ofrece retroalimentación oral a partir de la rúbrica, destacando la calidad del análisis de riesgos, la secuencia de acciones, la asignación de responsabilidades, la seguridad de los procedimientos y la capacidad de

mejora. Señala ejemplos concretos del desempeño, como “aislaron el equipo antes de intentar reparar” o “definieron una comunicación clara para los usuarios”. Cada grupo escribe una acción de mejora futura en su portafolio.

Transferencia y tarea

El docente relaciona el aprendizaje con el trabajo profesional: antes de intervenir un equipo, un técnico debe conocer el impacto de la falla, proteger los datos, documentar las acciones y saber cuándo escalar el incidente. Como reto de transferencia, los estudiantes pueden adaptar el plan a un aula de informática de su institución o a un pequeño negocio, sin utilizar datos personales ni intervenir equipos reales sin autorización. Deben agregar inventario básico, responsables y frecuencia de revisión.

Evaluación

Estrategia de evaluación

Tipo y momentos de evaluación

- **Diagnóstica:** Se aplica en la Fase de Inicio de la Sesión 1, durante la pregunta detonadora sobre los diez computadores que no encienden. Permite identificar conocimientos previos sobre diagnóstico, seguridad, prioridad y respaldo.
- **Formativa:** Se aplica durante la Actividad 1, la Actividad 2, el primer borrador, la construcción de procedimientos y la simulación. El docente utiliza preguntas guía, observación directa y revisión de productos parciales.
- **Sumativa:** Se aplica en el cierre de la Sesión 2 mediante la evaluación del plan de contingencia final, el desempeño en la simulación, la presentación breve y la reflexión individual.

Criterios de evaluación vinculados con los objetivos

- **Identificación de componentes:** Reconoce e integra en el documento los componentes esenciales de un plan de contingencia: riesgos, alcance, activación, responsables, recursos, comunicación, respuesta, recuperación y mejora. Vinculado con el objetivo 1.
- **Análisis y priorización de riesgos:** Relaciona causas, consecuencias, impacto y probabilidad, justificando técnicamente la prioridad de atención. Vinculado con el objetivo 2.
- **Diseño del plan:** Presenta procedimientos claros, ordenados, viables y seguros, con responsables, recursos, tiempos, criterios de escalamiento y evidencias de cierre. Vinculado con el objetivo 3.
- **Aplicación técnica:** Durante la simulación, protege la información, realiza un diagnóstico inicial, comunica el incidente, decide cuándo escalar y propone acciones de recuperación. Vinculado con el objetivo 4.
- **Evaluación y mejora:** Utiliza la retroalimentación de pares y del docente para corregir inconsistencias, mejorar la claridad y justificar los cambios realizados. Vinculado con el objetivo 5.

Instrumentos sugeridos

- **Rúbrica analítica:** Para valorar el plan final con niveles de desempeño: inicial, básico, competente y destacado.
- **Lista de cotejo:** Para verificar la presencia de componentes, la secuencia de acciones, la asignación de roles y las medidas de seguridad.
- **Guía de observación:** Para registrar el desempeño durante la simulación de contingencia.
- **Portafolio de proyecto:** Incluye matriz de riesgos, organizador gráfico, borrador, procedimientos, registro de simulación y versión final.
- **Coevaluación:** Cada grupo revisa el plan de otro equipo mediante dos fortalezas y dos recomendaciones concretas.
- **Autoevaluación:** Respuestas individuales a las preguntas metacognitivas del cierre.

Evidencias de aprendizaje

- **Objetivo 1:** Organizador gráfico y plan final con los componentes esenciales claramente diferenciados.
- **Objetivo 2:** Matriz de riesgos con valoración de impacto, probabilidad, consecuencias y prioridades justificadas.
- **Objetivo 3:** Documento del plan de contingencia con procedimientos de prevención, respuesta, recuperación, comunicación y mejora.
- **Objetivo 4:** Desempeño observable en la simulación, registro del incidente y diagrama de decisiones.
- **Objetivo 5:** Versión final corregida, recomendaciones de pares y registro escrito de los cambios realizados.

Ponderación sugerida

- Matriz de riesgos y análisis del caso: 20 %.
- Plan de contingencia final: 40 %.
- Simulación y aplicación del procedimiento: 25 %.
- Coevaluación, autoevaluación y reflexión metacognitiva: 15 %.