

Protege tus Datos: Caso Real para Entender la Protección de Datos Personales

Tecnología e Informática | Pensamiento Computacional | Aprendizaje Basado en Casos

Descripción

En este plan de clase, los estudiantes de media (15-17 años) explorarán el tema de la protección de datos personales a través de un enfoque práctico y cercano a su vida cotidiana. Aprenderán qué son los datos personales, por qué es crucial cuidarlos y cómo evitar riesgos comunes al compartir información en redes sociales y plataformas digitales. A partir del análisis de un caso real donde se vulneró la privacidad de un joven, desarrollarán habilidades críticas para identificar amenazas, tomar decisiones informadas y aplicar buenas prácticas de seguridad digital. Esta experiencia conecta directamente con su entorno digital habitual, incentivando la reflexión sobre su responsabilidad en la gestión de sus propios datos y los de otros. Así, el aprendizaje no solo es teórico, sino una herramienta para proteger su identidad y reputación en el mundo digital actual.

Objetivos de Aprendizaje

- Analizar un caso real de vulneración de datos personales para identificar riesgos y consecuencias.
- Argumentar la importancia de proteger la información personal en entornos digitales.
- Diseñar estrategias prácticas para salvaguardar datos personales en redes sociales y aplicaciones.
- Evaluar decisiones relacionadas con el manejo de datos para promover hábitos seguros en línea.

Recursos Necesarios

- Computadoras o tablets con acceso a internet (1 por estudiante o por pareja)
- Proyector y computadora del docente para mostrar videos y presentación
- Video corto sobre protección de datos personales (máximo 3 minutos)
- Impresiones del caso real resumido (1 copia por grupo de 3-4 estudiantes)
- Hojas de trabajo con preguntas guía para análisis del caso (1 por estudiante)
- Pizarrón o rotafolio y marcadores
- Plantillas para mapa mental o esquema (impresas o digitales)

Requisitos Previos

- Conocimiento básico sobre uso responsable de redes sociales y dispositivos digitales
- Experiencia previa en identificar información personal en plataformas digitales
- Habilidades básicas para trabajar en equipo y expresar opiniones oralmente

Actividades

Fase de Inicio

Tiempo estimado: 10 minutos

Propósito de la sesión

Docente: Explica que hoy explorarán cómo proteger sus datos personales, un tema clave para cuidar su privacidad y seguridad en internet, y que usarán un caso real para entenderlo mejor.

Estudiantes: Escuchan y se preparan para participar activamente.

Activación de conocimientos previos

Docente: Realiza la pregunta detonadora: “¿Qué tipo de información personal han compartido alguna vez en redes sociales o mensajes? ¿Creen que toda esa información es segura?” Pide que algunos estudiantes respondan brevemente.

Estudiantes: Comparten ejemplos de información que han publicado o recibido y reflexionan sobre riesgos posibles.

Motivación y enganche

Docente: Presenta un dato curioso: “¿Sabían que en promedio, cada persona tiene más de 100 datos personales circulando en internet? Un mal uso puede causar problemas reales.” Muestra un breve video que ejemplifica un caso de robo de identidad.

Estudiantes: Observan el video con atención y toman nota mental para el análisis posterior.

Contextualización

Docente: Conecta el tema con su realidad: “Como jóvenes, están muy activos en redes sociales y aplicaciones; aprender a proteger sus datos les ayudará a evitar situaciones incómodas o peligrosas.”

Estudiantes: Comprenden la relevancia y se preparan para profundizar en el tema.

Fase de Desarrollo

Tiempo estimado: 40 minutos

Presentación del contenido

Docente: Introduce un caso real adaptado: “Juan, un estudiante como ustedes, compartió en su perfil muchas fotos y datos personales. Un día, alguien usó esa información para hacerle una broma pesada que afectó su reputación y seguridad.” Distribuye la descripción resumida del caso a cada grupo.

Estudiantes: Reciben el caso y se preparan para analizarlo.

Actividad 1: Análisis del caso

- **Objetivo:** Analizar un caso real para identificar riesgos y consecuencias (Objetivo 1)

- **Instrucciones:** En grupos de 3-4, leen el caso y responden las preguntas guía:
 - ¿Qué datos personales compartió Juan?
 - ¿Qué riesgos enfrentó por esa información pública?
 - ¿Qué consecuencias tuvo para él y su entorno?
- **Organización:** Grupos de 3-4 estudiantes
- **Producto:** Respuestas escritas en hoja de trabajo
- **Tiempo:** 15 minutos
- **Rol docente:** Circula entre grupos, fomenta la discusión con preguntas como “¿Creen que Juan podía evitar esto? ¿Cómo?” y ayuda a clarificar conceptos.

Actividad 2: Debate argumentativo

- **Objetivo:** Argumentar la importancia de proteger la información personal (Objetivo 2)
- **Instrucciones:** En plenaria, cada grupo expone sus conclusiones y se debate sobre:
 - ¿Por qué es importante cuidar nuestros datos personales?
 - ¿Qué hábitos digitales podrían cambiar para protegerse mejor?
- **Organización:** Plenaria
- **Producto:** Lista colectiva en el pizarrón de buenas prácticas y riesgos comunes
- **Tiempo:** 12 minutos
- **Rol docente:** Modera el debate, invita a escuchar y respetar opiniones, sintetiza ideas clave en el pizarrón.

Actividad 3: Diseño de estrategias personales

- **Objetivo:** Diseñar estrategias prácticas para proteger datos personales (Objetivo 3)
- **Instrucciones:** Individualmente, cada estudiante completa una plantilla donde escribe al menos tres acciones concretas que implementará para cuidar su información en redes y aplicaciones.
- **Organización:** Individual
- **Producto:** Plantilla con estrategias personales
- **Tiempo:** 10 minutos
- **Rol docente:** Apoya a quienes tienen dudas, sugiere ideas si es necesario, revisa algunas respuestas para retroalimentar.

Diferenciación

- **Para estudiantes que terminan antes:** Proponer que creen un breve mensaje o post para redes sociales que invite a sus amigos a proteger sus datos.
- **Para estudiantes que requieren más apoyo:** Brindar ejemplos concretos adicionales y trabajar en pareja con guía directa del docente.

Transiciones

Docente: Conecta el análisis del caso con el debate explicando que “Ahora que entendimos el problema, vamos a compartir nuestras ideas para prevenirlo y diseñar soluciones prácticas”. Luego, antes del diseño personal dice: “Finalmente, vamos a pensar en qué podemos hacer cada uno para cuidarnos.”

Fase de Cierre

Tiempo estimado: 10 minutos

Síntesis

Docente: Pide a los estudiantes que en pareja elaboren un resumen en 3 ideas clave sobre la protección de datos personales basadas en lo aprendido hoy, usando una hoja o pizarra pequeña.

Estudiantes: Escriben y comparten sus ideas con el grupo.

Reflexión metacognitiva

Docente: Formula estas preguntas para que escriban en sus cuadernos:

- ¿Qué aprendí sobre los riesgos de compartir datos personales?
- ¿Cómo puedo aplicar hoy mismo lo que aprendí para proteger mi información?
- ¿Qué duda o inquietud tengo sobre el tema?

Retroalimentación

Docente: Recoge algunas respuestas y comenta en voz alta reforzando los aciertos y aclarando dudas comunes. Felicita la participación y el compromiso.

Transferencia

Docente: Invita a que en casa observen cómo sus familiares manejan sus datos personales y compartan con ellos lo aprendido. Explica que esta reflexión es importante para su seguridad digital continua.

Tarea o reto

Docente: Propone el reto voluntario de crear un “manual familiar de buenas prácticas para proteger datos” y llevarlo a la siguiente clase para compartir experiencias.

Estudiantes: Reciben el reto con motivación y preparan la tarea en casa.

Evaluación

Tipo de evaluación: Diagnóstica al inicio con la pregunta detonadora; formativa durante el análisis del caso, debate y diseño de estrategias; sumativa en la síntesis y reflexión final.

Criterios de evaluación:

- Identifica correctamente riesgos y consecuencias en el análisis del caso (Objetivo 1)
- Argumenta de forma clara y fundamentada la importancia de proteger datos personales (Objetivo 2)

- Diseña estrategias prácticas y aplicables para la protección de datos (Objetivo 3)
- Reflexiona sobre su aprendizaje y plantea acciones concretas para mejorar su seguridad digital (Objetivo 4)

Instrumentos sugeridos:

- Lista de cotejo para observar participación en actividades grupales y debate
- Revisión de respuestas escritas en hoja de trabajo y plantilla de estrategias
- Autoevaluación escrita de la reflexión metacognitiva
- Observación directa durante actividades y retroalimentación oral

Evidencias de aprendizaje:

- Respuestas al análisis del caso
- Conclusiones y aportes en el debate
- Plantilla con estrategias personales para proteger datos
- Resumen en 3 ideas clave y respuestas de reflexión metacognitiva