

Protege tu Huella Digital: Privacidad y Seguridad en el Mundo Digital

Tecnología e Informática | Pensamiento Computacional | Diseño Universal para el Aprendizaje

Descripción

En esta sesión de Pensamiento Computacional, los estudiantes explorarán los conceptos fundamentales de privacidad de la información y seguridad digital, temas esenciales en la era de la conectividad constante. Aprenderán a identificar riesgos asociados al manejo de datos personales y a aplicar buenas prácticas para proteger su huella digital. La relevancia de este tema radica en que, a diario, los jóvenes interactúan con múltiples plataformas digitales que recopilan y utilizan su información, lo que puede afectar su seguridad y reputación si no se maneja adecuadamente. Además, desarrollarán competencias para analizar situaciones reales y tomar decisiones informadas que garanticen su protección en línea. Este aprendizaje conecta directamente con su vida cotidiana, ya que les permitirá navegar el entorno digital de manera responsable y segura, evitando fraudes, suplantación de identidad y otros riesgos digitales. La metodología del Diseño Universal para el Aprendizaje asegura que todos los estudiantes, con diferentes estilos y necesidades, accedan y participen activamente en el proceso de aprendizaje.

Objetivos de Aprendizaje

- Analizar los conceptos de privacidad de la información y seguridad digital en contextos cotidianos.
- Identificar riesgos comunes relacionados con la exposición de datos personales en línea.
- Aplicar estrategias prácticas para proteger la información personal en plataformas digitales.
- Argumentar la importancia de la privacidad digital para el bienestar individual y social.

Recursos Necesarios

- Computadora o tablet con acceso a internet (1 por estudiante o pareja).
- Proyector y computadora para presentación multimedia.
- Video educativo corto sobre privacidad y seguridad digital (3-5 minutos).
- Hoja impresa con situaciones problemáticas para análisis (1 por estudiante).
- Carteles con definiciones clave de privacidad y seguridad digital.
- Formulario digital o papel para "Ticket de salida".
- Aplicación o herramienta para crear mapas mentales (ej. Coggle, MindMeister) o papel y marcadores.

Requisitos Previos

- Conocimientos básicos sobre uso de internet y redes sociales.

- Experiencia previa con plataformas digitales comunes (redes sociales, mensajería instantánea).
- Habilidades básicas para buscar información en línea y trabajar en equipo.

Actividades

Fase de Inicio

Tiempo estimado: 10 minutos

Propósito de la sesión

Docente: Explica a los estudiantes que en esta sesión explorarán cómo proteger su información personal en internet y por qué esta habilidad es clave para su seguridad y privacidad en el mundo digital actual.

Activación de conocimientos previos

Docente: Inicia con la pregunta detonadora: “¿Alguna vez compartiste información personal en internet y luego te arrepentiste? ¿Qué pasó?”

Estudiantes: Responden brevemente compartiendo experiencias o ideas en voz alta en plenaria.

Motivación y enganche

Docente: Presenta un dato curioso: “Cada día se envían más de 306 mil millones de correos electrónicos. ¿Sabías que el 45% de los usuarios nunca cambian sus contraseñas? Esto puede poner en riesgo tu información.”

Estudiantes: Reflexionan sobre el dato y expresan opiniones rápidas sobre la seguridad de sus contraseñas.

Contextualización

Docente: Conecta el tema con su vida diaria: “Ustedes usan redes sociales, aplicaciones y juegos que piden datos personales. Aprender a proteger esa información es protegerse a ustedes mismos.”

Estudiantes: Escuchan y anotan ideas principales para recordar el propósito de la sesión.

Fase de Desarrollo

Tiempo estimado: 40 minutos

Presentación del contenido

Docente: Muestra un video educativo corto que explica conceptos básicos de privacidad y seguridad digital, incluyendo ejemplos de riesgos comunes como phishing, contraseñas débiles y exposición en redes sociales.

Estudiantes: Observan el video y toman notas sobre aspectos importantes.

Actividad 1: Identificando riesgos en situaciones reales

- **Objetivo:** Identificar riesgos comunes relacionados con la exposición de datos personales en línea.

- **Instrucciones:**

- El docente entrega a cada estudiante una hoja con 4 situaciones problemáticas donde se expone información personal en internet.
- Los estudiantes leen individualmente cada situación y subrayan los riesgos que detectan.
- Luego, en grupos de 3-4, discuten sus respuestas y elaboran un listado breve de riesgos comunes.
- Finalmente, cada grupo comparte en plenaria un riesgo identificado y cómo podría evitarse.

- **Organización:** Individual y grupos pequeños.

- **Producto:** Listado de riesgos comunes y propuestas de prevención.

- **Tiempo:** 15 minutos.

- **Rol docente:** Circula entre grupos, formula preguntas guía como “¿Qué consecuencias podría tener esta situación?” o “¿Cómo cambiarías esta acción para proteger la información?”

Transición

Docente: Resume los riesgos identificados y conecta con la siguiente actividad: “Ahora vamos a pensar en cómo protegernos usando estrategias concretas para cuidar nuestra privacidad.”

Actividad 2: Creando un plan personal de seguridad digital

- **Objetivo:** Aplicar estrategias prácticas para proteger la información personal en plataformas digitales.

- **Instrucciones:**

- En parejas, los estudiantes usan una plantilla digital o papel para diseñar un plan con al menos 5 acciones concretas para proteger su privacidad (ej. crear contraseñas seguras, configurar privacidad en redes sociales, evitar compartir datos sensibles).
- Investigan brevemente (en internet o con el docente) para enriquecer sus ideas.
- Preparan una breve explicación para compartir su plan con la clase.

- **Organización:** Parejas.

- **Producto:** Plan personal de seguridad digital escrito y explicado.

- **Tiempo:** 20 minutos.

- **Rol docente:** Facilita recursos, responde dudas, incentiva la reflexión con preguntas como “¿Cómo sabrás que esta acción funciona?” o “¿Qué harías si alguien intenta acceder a tu cuenta sin permiso?”

Diferenciación

- **Para estudiantes que terminan antes:** Se les invita a explorar configuraciones de privacidad en su dispositivo o red social favorita y compartir una recomendación adicional.
 - **Para estudiantes que requieren más apoyo:** El docente ofrece ejemplos concretos y apoyo guiado durante la creación del plan, usando preguntas específicas y mapas conceptuales impresos.
-

Fase de Cierre

Tiempo estimado: 10 minutos

Síntesis

Docente: Solicita a cada estudiante escribir en un "Ticket de salida" tres ideas claves que aprendieron sobre privacidad y seguridad digital y una acción que se comprometen a realizar para proteger su información.

Estudiantes: Plasman sus respuestas en el formulario digital o en hoja entregada.

Reflexión metacognitiva

Docente: Plantea las siguientes preguntas para reflexión oral rápida o escrita:

- ¿Cómo puedo aplicar lo aprendido para proteger mis datos en internet?
- ¿Qué riesgos nuevos puedo identificar ahora que antes no veía?
- ¿Por qué es importante cuidar mi privacidad digital para mi bienestar?

Retroalimentación

Docente: Recolecta los tickets, comenta algunas respuestas destacadas en plenaria, corrige dudas comunes y refuerza puntos clave con mensajes positivos y claros.

Transferencia

Docente: Anima a los estudiantes a compartir lo aprendido con su familia y amigos para fomentar una cultura de seguridad digital y anticipa que en próximas sesiones explorarán herramientas tecnológicas para reforzar estas prácticas.

Tarea o reto

Docente: Propone un reto: "Durante esta semana, revisa las configuraciones de privacidad de una de tus redes sociales o aplicaciones y ajusta al menos una opción para mejorar tu seguridad. Anota qué cambiaste y cómo te sentiste al hacerlo."

Estudiantes: Se comprometen a realizar el reto y traerán sus experiencias para compartir en la siguiente clase.

Evaluación

Tipo de evaluación:

- **Diagnóstica:** En la fase de inicio, con la pregunta detonadora para conocer conocimientos previos sobre privacidad y experiencias personales.
- **Formativa:** Durante el desarrollo, mediante la observación de la identificación de riesgos y la elaboración del plan personal de seguridad digital.
- **Sumativa:** En el cierre, con el "Ticket de salida" y la reflexión metacognitiva que muestran comprensión y aplicación del tema.

Criterios de evaluación:

- Capacidad para identificar riesgos de privacidad en situaciones digitales (objetivo 2).
- Aplicación de estrategias concretas para proteger la información personal (objetivo 3).
- Argumentación clara sobre la importancia de la privacidad digital (objetivo 4).
- Participación activa en actividades grupales e individuales (objetivo 1).

Instrumentos sugeridos:

- Lista de cotejo para observar la participación y comprensión durante actividades grupales.
- Rúbrica para evaluar el plan personal de seguridad digital considerando claridad, relevancia y aplicabilidad.
- Revisión de los "Tickets de salida" para valorar síntesis y compromiso.
- Observación directa y registro anecdótico durante la reflexión y discusión.

Evidencias de aprendizaje:

- Listado de riesgos identificados en situaciones problemáticas.
- Plan personal de seguridad digital desarrollado en parejas.
- Respuestas en el "Ticket de salida" que muestran comprensión y compromiso.
- Participación y aportaciones en discusiones y reflexiones grupales.