Actividad 8: Diálogo Abierto

Navegando entre desinformación y Fakenews: estrategias para educar con pensamiento crítico

Vinculación Curricular
Curso: 3° Medio.
Asignatura: Ciencias para la Ciudadanía, Módulo Semestral: Tecnología y Sociedad.
Unidad 1: Innovación tecnológica: ¿Hasta dónde llegaremos?

Google for Education
CENTRO DE INNOVACIÓN MINISTERIO DE EDUCACIÓN
DigiMENTE

Este material fue desarrollado en colaboración con el Centro de Innovación del Ministerio de Educación de Chile, en el marco del convenio con Google for Education (DEX 1451 de 2023)

2025

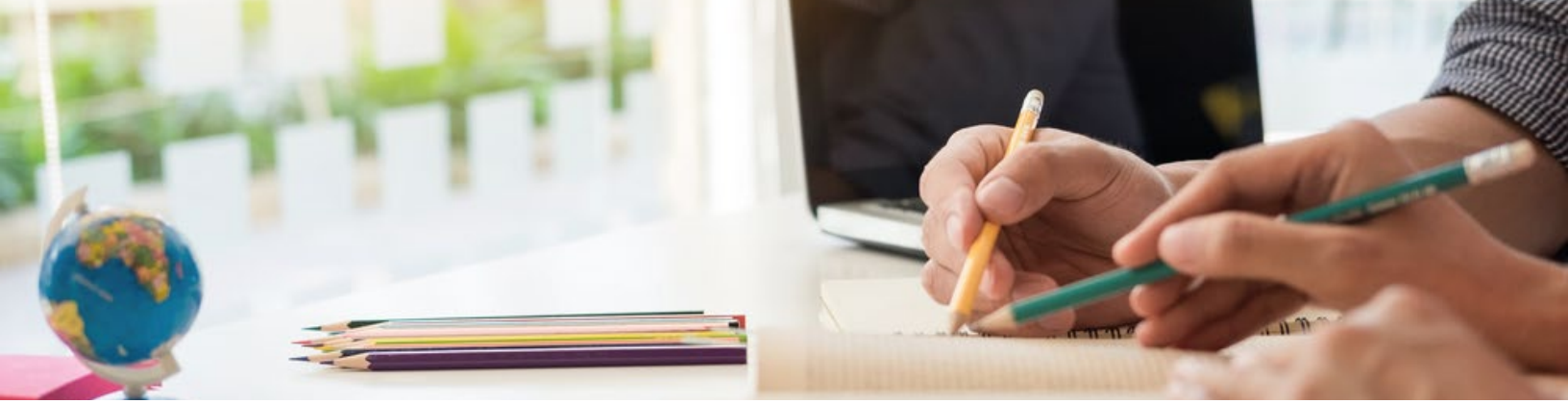
Actividad

Diálogo abierto

La guía ayuda a las y los docentes a estructurar actividades que complementen el desarrollo del OA3 de las unidad 1: "Innovación tecnológica: hasta donde llegaremos? al fomentar el pensamiento crítico y la participación de las y los estudiantes. A través de estrategias prácticas, facilita el análisis de información y la conexión con situaciones reales, promoviendo una comprensión más reflexiva y aplicada de los contenidos.

Propósito

Desarrollar en las y los estudiantes una comprensión crítica sobre la privacidad digital, permitiéndoles identificar riesgos, evaluar el impacto de las configuraciones de seguridad en redes sociales y aplicaciones, y proponer estrategias efectivas para la protección de su información personal. Esto fortalecerá su capacidad de tomar decisiones informadas y responsables en entornos digitales.



Objetivos de aprendizaje:

OA3	Evaluar alcances y limitaciones de la tecnología digital y sus aplicaciones, argumentando riesgos y beneficios desde una perspectiva de salud, ética, social, económica y ambiental.
OA a.	Formular preguntas y problemas sobre tópicos científicos de interés, a partir de la observación de fenómenos y/o la exploración de diversas fuentes.
OA b.	Planificar y desarrollar investigaciones que permitan recoger evidencias y contrastar hipótesis, con apoyo de herramientas tecnológicas y matemáticas.
OA e.	Construir, usar y comunicar argumentos científicos.
OA i.	Analizar críticamente implicancias sociales, económicas, éticas y ambientales de problemas relacionados con controversias públicas que involucran ciencia y tecnología digital.

Criterios de evaluación:

- Analizan la privacidad digital mediante la identificación de riesgos y estrategias de protección.
- Argumentan sobre la tecnología digital justificando sus posturas con evidencia y casos reales.
- Participan reflexivamente en diálogos sobre privacidad digital, considerando diversas perspectivas.

Actitud: Valorar las TIC como una oportunidad para informarse, investigar, socializar, comunicarse y participar como ciudadano.

Tema prioritario: Inteligencia artificial y seguridad digital.

Duración (90 min)

Desarrollo:

Observar el video **Cápsula alfabetización digital crítica y reflexiva**.

Observaciones al docente *Explicar a los estudiantes los términos esenciales sobre el tema* **15 minutos**

La inteligencia artificial (IA) está cada vez más presente en nuestra vida cotidiana, integrándose en redes sociales, plataformas de compras, asistentes virtuales y muchas otras aplicaciones. Su capacidad para analizar grandes volúmenes de datos y tomar decisiones automatizadas ha transformado la manera en que nos comunicamos, trabajamos y consumimos información. Sin embargo, a medida que esta tecnología digital avanza, también surgen debates sobre sus alcances y limitaciones, así como sobre los riesgos y beneficios que implica su uso.

Desde una perspectiva ética y social, la IA puede generar preocupaciones sobre la privacidad digital, la desinformación y el sesgo en los algoritmos. Económicamente, impulsa la eficiencia en diversas industrias, pero también plantea desafíos en el mercado laboral debido a la automatización. En términos de salud, se utiliza para mejorar diagnósticos médicos y tratamientos, pero su mal uso podría comprometer la seguridad de la información personal. Ambientalmente, la IA contribuye a optimizar el uso de recursos, aunque el procesamiento de datos a gran escala puede aumentar el consumo energético.

Dado su impacto en múltiples aspectos de la sociedad, es fundamental evaluar de manera crítica los beneficios y riesgos de la inteligencia artificial. En este contexto, es clave comprender cómo funciona, qué implicaciones tiene para nuestra privacidad y cómo podemos utilizarla de manera responsable para maximizar sus ventajas y reducir sus efectos negativos.

Conceptos Claves

- **Privacidad Digital:** Es el derecho a proteger los datos personales y decidir cómo se utilizan. Ejemplo: Al comprar en línea, proporcionar un número de teléfono puede exponernos a publicidad no deseada.
- **Algoritmos de IA:** Son procesos que permiten a los sistemas aprender automáticamente según los datos que reciben. Ejemplo: TikTok recomienda contenido sobre deportes si frecuentemente se interactúa con videos relacionados.
- **Amenazas a la privacidad:** Exposición o uso no autorizado de datos, como el rastreo de ubicación o acceso a micrófonos. Ejemplo: En Snapchat, compartir la ubicación sin configuraciones adecuadas puede comprometer la privacidad.

- **Smishing** es un tipo de estafa en la que los ciberdelincuentes utilizan **mensajes de texto (SMS)** o **aplicaciones de mensajería** para engañar a las personas y hacer que revelen información personal, como contraseñas, datos bancarios o credenciales de acceso. Conoce cómo funciona este tipo de estafa digital:
- **Mensaje fraudulento:** Recibes un SMS que parece provenir de un banco, una empresa de mensajería, una red social u otra entidad confiable.
- **Llamado a la acción urgente:** El mensaje suele incluir una alerta de seguridad falsa, una oferta especial o una solicitud para confirmar información.
- **Enlace o número de teléfono fraudulento:** El mensaje contiene un enlace que dirige a una página web falsa o te pide que llames a un número donde intentarán obtener tus datos.
- **Robo de información:** Si ingresas tus datos en la página falsa o interactúas con los estafadores, pueden robar tu información personal o instalar malware en tu dispositivo.

Ejemplos en la Vida Diaria:

- ***Redes Sociales:*** Analizan las interacciones para ofrecer contenido personalizado.
- ***Asistentes Virtuales:*** Aplicaciones como Siri utilizan IA para ejecutar comandos.
- ***Aplicaciones de compras en línea:*** Plataformas como Amazon o Mercado Libre recomiendan productos basándose en el historial de búsqueda y compras previas.

Analizando Casos Reales

15 minutos

Resolver una serie de desafíos cortos que deben discutir y encontrar soluciones antes de pasar al siguiente desafío.

Desafío 1: Mensaje Sospechoso en Redes Sociales
Un/a estudiante recibe un mensaje en Instagram de una cuenta desconocida con un enlace diciendo que ha ganado un premio.

Pregunta: ¿Qué señales pueden indicar que este mensaje es un intento de fraude?
Si se detecta que esto es una estafa digital, smishing, ¿Qué implicaciones podría tener en la salud, ética, entorno social y económico del estudiante y su círculo cercano?

Desafío 2: Configuración de Privacidad en una Aplicación
Al instalar una app nueva, pide acceso a la cámara, micrófono, contactos y ubicación.

Pregunta: ¿Cuáles de estos permisos deberían revisarse antes de aceptarlos y por qué?

Desafío 3: Publicidad Basada en IA
Después de hablar sobre un videojuego con un amigo, un/a estudiante nota que en su celular aparecen anuncios del juego.

Pregunta: ¿Cómo ocurre esto y qué medidas pueden tomarse para controlar este tipo de seguimiento?

Observaciones a las y los docentes:

- *Es importante guiar la dinámica asegurando que los equipos avancen de manera ágil y resuelvan cada desafío en **máximo 3 minutos**. Si algún grupo se queda atascado, se pueden formular preguntas adicionales como: "¿Han recibido mensajes similares en sus redes sociales?", "¿Qué configuraciones de privacidad han revisado en sus aplicaciones?" o "¿Han notado publicidad de algo que solo hablaron en voz alta?". Estas preguntas ayudarán a conectar la actividad con experiencias personales y hacer que las y los estudiantes reflexionen sobre su propia privacidad digital.*

- *En el primer desafío, donde las y los estudiantes analizan un **mensaje sospechoso en redes sociales**, deben identificar señales de advertencia como nombres de usuario extraños o recién creados, errores ortográficos o gramaticales, enlaces acortados o desconocidos, y promesas poco creíbles, como ganar un premio sin haber participado en un concurso. Las medidas de protección esperadas incluyen no hacer clic en enlaces desconocidos, no responder ni compartir datos personales, reportar y bloquear la cuenta sospechosa, y activar la autenticación en dos pasos en redes sociales para mayor seguridad.*

- *En el segundo desafío, sobre **configuración de privacidad en una aplicación**, las y los estudiantes deben identificar qué permisos son riesgosos o innecesarios. Se espera que reconozcan que la ubicación solo debe activarse si es esencial para la función de la app (como en mapas), que el acceso al micrófono y la cámara debe limitarse a aplicaciones que realmente lo necesiten, y que el permiso de contactos no debe concederse sin revisar su propósito. Para proteger sus datos, las y los estudiantes deben aprender a revisar y ajustar estos permisos en la configuración del celular, usar versiones web en lugar de aplicaciones cuando sea posible y leer los términos de privacidad antes de instalar una nueva app.*

- *En el tercer desafío, sobre **publicidad basada en IA**, las y los estudiantes deben entender que los dispositivos utilizan algoritmos de inteligencia artificial para analizar búsquedas, interacciones y, en algunos casos, el uso del micrófono para personalizar anuncios. Empresas como Google y Meta recopilan datos de navegación para ofrecer publicidad dirigida. Para mejorar su privacidad, las y los estudiantes pueden desactivar la personalización de anuncios en la configuración de privacidad, limitar el acceso al micrófono para aplicaciones que no lo necesitan y borrar regularmente cookies y caché en sus navegadores.*

Reflexionando 10 minutos

En un Google Doc o en una hoja en blanco, las y los estudiantes investigan consultando fuentes confiables como artículos científicos publicados en revistas especializadas o por Universidades de prestigio u organizaciones internacionales y escriben su respuesta a las siguientes preguntas:

- "¿Cómo influye la IA en nuestra vida cotidiana? ¿Qué riesgos creen que tiene sobre la privacidad personal, así como implicancias sociales, económicas, éticas y ambientales? Recuerden buscar ejemplos del día a día, como las aplicaciones que usan en el celular, las redes sociales o el uso del micrófono en los asistentes virtuales.

Observaciones a las y los docentes:

- *Recordar a las y los estudiantes que estructuren sus respuestas usando argumentos científicos y citando fuentes confiables de información. La estructura sugerida es: introducción integrando datos cuantitativos o cualitativos resultados de la investigación(explicación general sobre la IA), desarrollo (ejemplos específicos citando artículos científicos y sus riesgos) y conclusión (reflexión sobre su postura frente al tema).*
- *Animar a las y los estudiantes a usar términos clave, como "huella digital", "protección de datos", "algoritmos de recomendación" y "consentimiento informado".*

Compartiendo Ideas 20 minutos

Formar grupos de 3 a 4 personas para compartir lo que escribieron en la reflexión y conversar sobre:

- ¿Qué beneficios aporta el uso de la IA y qué riesgos se presentan para la privacidad digital?
- ¿Cómo se puede proteger los datos personales mientras se usan tecnologías digitales que involucran IA?

Observaciones a las y los docentes:

- *Facilitar el trabajo en grupos asegurándose de que cada estudiante tenga un rol, como moderador/a, relator/a o encargado/a de registrar conclusiones.*
- *Proporcionar ejemplos de estrategias para la protección de datos personales, como el uso de contraseñas seguras, configuración de privacidad en aplicaciones y uso de navegadores que respeten la privacidad.*
- *Escuchar las discusiones y, si es necesario, hacer preguntas guía, por ejemplo: ¿Cómo influye la regulación de datos en estos casos? o ¿Qué cambios harían en las políticas de privacidad de sus aplicaciones favoritas?*

Registrando 15 minutos

Después de la discusión grupal, registrar en el archivo de Google Docs o en la hoja en blanco en la que están trabajando:

- Beneficios que la IA trae a nuestra vida diaria.
- Principales riesgos sobre la privacidad digital que se discutieron.
- Soluciones para proteger la privacidad mientras usamos aplicaciones y s digitales con IA.

Observaciones a las y los docentes:

- *Proporcionar una estructura clara para el registro de ideas, sugiriendo que cada punto tenga una breve explicación y al menos un ejemplo.*
- *Revisar que las soluciones propuestas sean realistas y aplicables. En caso de que no lo sean, pedir a las y los estudiantes que lo realicen, por ejemplo: en lugar de "tener más seguridad", preguntar ¿qué medidas específicas mejorarían la seguridad?*
- *Fomentar el uso de fuentes confiables para respaldar sus argumentos. Pueden consultar políticas de privacidad de aplicaciones populares o estudios sobre IA y privacidad.*

Concluyendo 10 minutos

Ahora de forma individual, reflexionan sobre las siguientes preguntas:

- ¿Qué medidas tomarían para proteger sus datos personales cuando usan tecnología digital con IA?
- ¿Cuál es el principal riesgo que perciben sobre la privacidad digital en su vida diaria?

Observaciones a las y los docentes:

Utilizar esta reflexión final como una forma de evaluar cómo han comprendido los riesgos y las soluciones para proteger la privacidad en la era digital, considerando:

- *Pedir a las y los estudiantes que expliquen cómo aplicarían las medidas de protección en su propia vida digital, asegurándose de que sus respuestas sean prácticas y no solo teóricas.*
- *Identificar si las y los estudiantes han cambiado su percepción sobre la privacidad digital tras la actividad, preguntando: ¿Piensan diferente sobre cómo usan sus datos en internet después de esta clase?*
- *Evaluar la profundidad de sus respuestas observando si incluyen ejemplos concretos, análisis de impacto y soluciones personales aplicables.*

Sugerencias de evaluación:

Criterios de Evaluación	**Nivel 1** Nivel Inicial	**Nivel 2** Nivel Básico	**Nivel 3** Nivel Avanzado	**Nivel 4** Nivel Experto
Analizan la privacidad digital mediante la identificación de riesgos y estrategias de protección.	No identifica riesgos en los casos analizados en la actividad "Analizando Casos Reales". No reconoce amenazas en la privacidad digital.	Identifica algunos riesgos en los casos de "Analizando Casos Reales", pero sin explicar claramente su impacto. Propone estrategias generales sin justificar su efectividad.	Analiza diversos riesgos de privacidad digital en la actividad "Analizando Casos Reales". Justifica estrategias de protección basándose en ejemplos concretos. Aplica conocimientos en la actividad de "Configuración de Privacidad".	Evalúa críticamente los riesgos en privacidad digital en "Analizando Casos Reales" y "Configuración de Privacidad". Diseña estrategias innovadoras y argumentadas para la protección de datos. Relaciona su análisis con tendencias actuales.
Argumentan sobre la digital justificando sus posturas con evidencia y casos reales.	No logra argumentar sobre los efectos de la IA en la actividad "Desafíos de Privacidad Digital". Sus ideas son vagas y sin sustento en ejemplos o evidencias.	Presenta una postura en "Desafíos de Privacidad Digital", pero con argumentos poco desarrollados o sin apoyo en casos reales.	Argumenta con ejemplos concretos los impactos de la IA y la tecnología digital en "Desafíos de Privacidad Digital" y "Publicidad Basada en IA". Justifica sus ideas con evidencias y casos reales.	Construye argumentos sólidos sobre la IA y la privacidad digital en "Desafíos de Privacidad Digital" y "Publicidad Basada en IA". Relaciona sus ideas con contextos actuales y propone soluciones innovadoras.
Participan reflexivamente en diálogos sobre privacidad digital, considerando diversas perspectivas.	No participa en el "Diálogo Abierto" ni en la discusión de "Ejemplos en la Vida Diaria". Sus aportes son mínimos y poco relevantes.	Participa de manera limitada en el "Diálogo Abierto", expresando ideas generales sin profundizar en diferentes perspectivas.	Expone sus ideas con claridad en el "Diálogo Abierto" y en la discusión de "Ejemplos en la Vida Diaria", considerando distintos puntos de vista y relacionándolos con la privacidad digital.	Participa activamente en el "Diálogo Abierto" y en "Ejemplos en la Vida Diaria", demostrando pensamiento crítico y considerando múltiples perspectivas. Relaciona el debate con implicaciones éticas y sociales.

Recursos y sitios web:

- Cápsula alfabetización digital crítica y reflexiva.
- Privacidad digital.
- Protección de datos en Chile en la era digital
- Guía de privacidad de los productos de Google
- Inteligencia artificial ¿Amiga o enemiga?
- Diplomado Educación híbrida: Módulo 2. Herramientas y aplicaciones para la transición de la educación híbrida.