Actividad 4: Redes Sociales y Privacidad

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

Vinculación Curricular
Curso: 8° Básico.
Asignatura: Tecnología.
Unidad: Planteamiento del problema e identificación de necesidades.

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

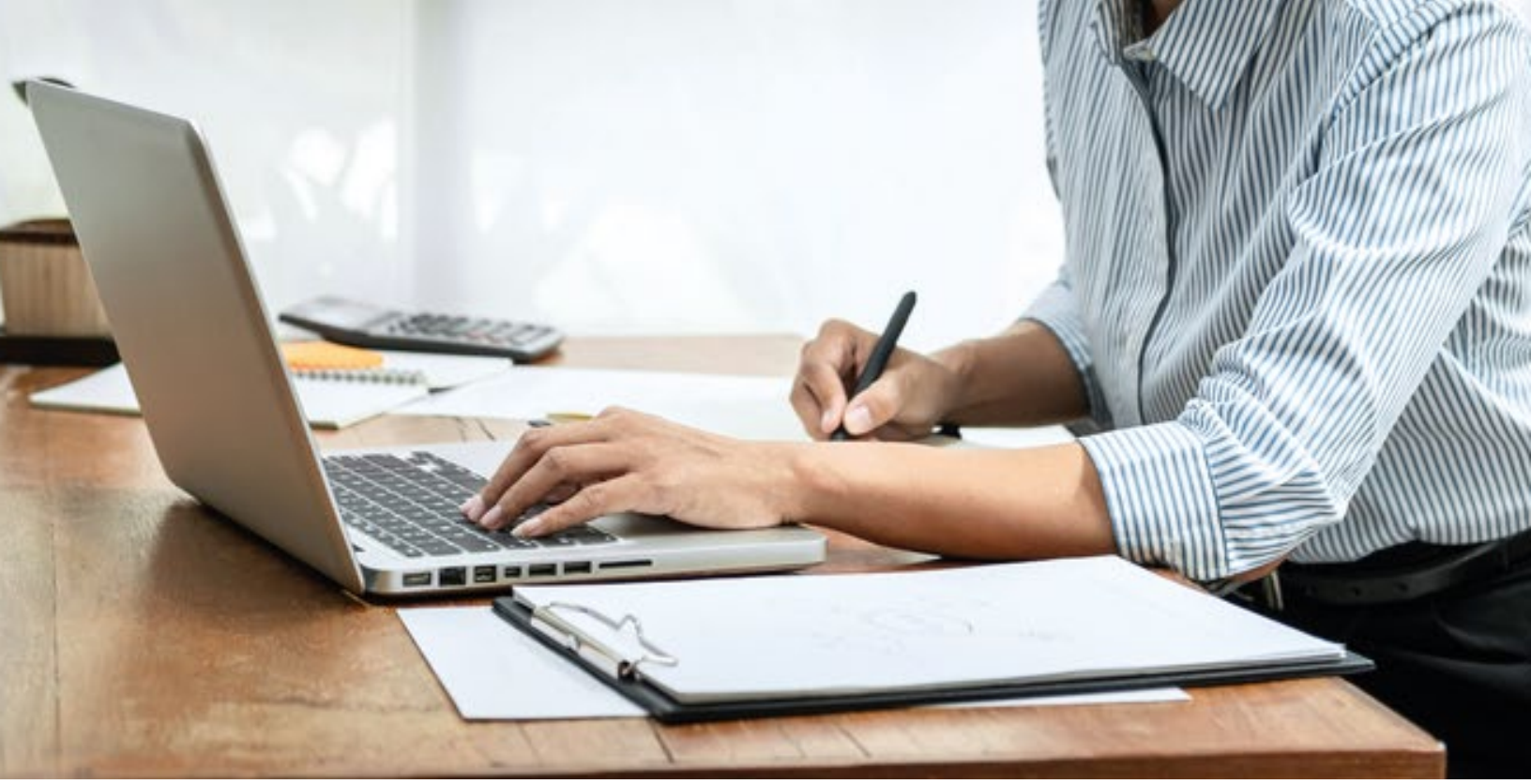
Actividad

Redes Sociales y Privacidad

Esta guía complementa las actividades del OA6 la Unidad 1: Planteamiento del problema e identificación de necesidades. A través de sus actividades, se fomenta el uso de plataformas digitales y la configuración de privacidad en redes sociales, permitiendo a las y los estudiantes explorar herramientas tecnológicas para gestionar su información personal de manera segura. Además, contribuye al desarrollo de habilidades para la toma de decisiones responsables en entornos digitales, promoviendo una actitud crítica y de autocuidado en el uso de las TIC.

Propósito

Desarrollar una comprensión crítica sobre la privacidad en redes sociales, identificando riesgos asociados al uso de plataformas digitales, explorando estrategias para proteger su información personal. A través del análisis de casos y la reflexión sobre sus propias prácticas en línea, fortalecerán su capacidad de tomar decisiones seguras y responsables en entornos digitales.



Objetivos de aprendizaje:

OA6	Explorar y usar una variedad de software educativos (simuladores, libros digitales, interactivos y creativos, entre otros) para lograr aprendizajes significativos y una interacción apropiada con las TIC.

Criterios de evaluación:

- Explican los aspectos éticos asociados a las diversas soluciones tecnológicas analizadas.
- Explican los aspectos sociales asociados a las diversas soluciones tecnológicas analizadas.
- Formulan medidas de mitigación que contemplen una descripción del proceso de producción de la solución tecnológica analizada.

Actitud: Demostrar disposición hacia la prevención de riesgos y el autocuidado, entendidos como la capacidad progresiva respecto de la valoración de la vida, el cuerpo, el bienestar y la salud, así como el desarrollo de prácticas y hábitos para mejorar la propia seguridad y la de los demás, y con ello prevenir riesgos.

Tema prioritario: Inteligencia artificial y seguridad digital.

Duración (90 min)

Desarrollo:

Observar el video **Cápsula alfabetización digital crítica y reflexiva**. 5 minutos

Observaciones a las y los docentes: Duración (20 min)

En la era digital, cada clic, publicación y dato compartido en línea deja una huella. Las redes sociales, las aplicaciones y las plataformas en la web nos ofrecen infinitas oportunidades para comunicarnos, aprender y expresarnos, pero también nos exponen a riesgos que muchas veces desconocemos. ¿Cuántas veces hemos aceptado términos y condiciones sin leerlos? ¿Sabemos realmente qué sucede con nuestra información una vez que la subimos a internet?

El acceso a la tecnología digital nos permite conectarnos con el mundo; sin embargo, conlleva una gran responsabilidad. No solo debemos proteger nuestros datos, sino también ser conscientes del impacto de nuestras acciones digitales en los demás y en el entorno. Compartir una foto sin consentimiento, difundir información sin verificar o almacenar datos de manera indiscriminada no solo afectan nuestra privacidad, sino que pueden contribuir a problemas más amplios como la desinformación o el impacto ambiental del uso de servidores y almacenamiento en la nube.

Por esta razón, es fundamental desarrollar una actitud crítica y reflexiva sobre nuestra presencia digital. A través de esta guía, aprenderemos a identificar los riesgos, aplicar buenas prácticas para la protección de datos personales y tomar decisiones informadas sobre el uso responsable de las tecnologías digitales. Así, no solo cuidaremos nuestra seguridad, sino que también contribuiremos a una ciudadanía digital más ética, respetuosa y sostenible.

Introducir el tema de redes sociales y privacidad con una base conceptual clara.

- **Privacidad digital en redes sociales:** Se refiere al control que cada persona tiene sobre su información en plataformas digitales y cómo esta se comparte o se utiliza. Muchas redes sociales recopilan datos personales para mejorar la experiencia de la persona usuaria, pero si no se gestionan bien, pueden exponer información sensible.

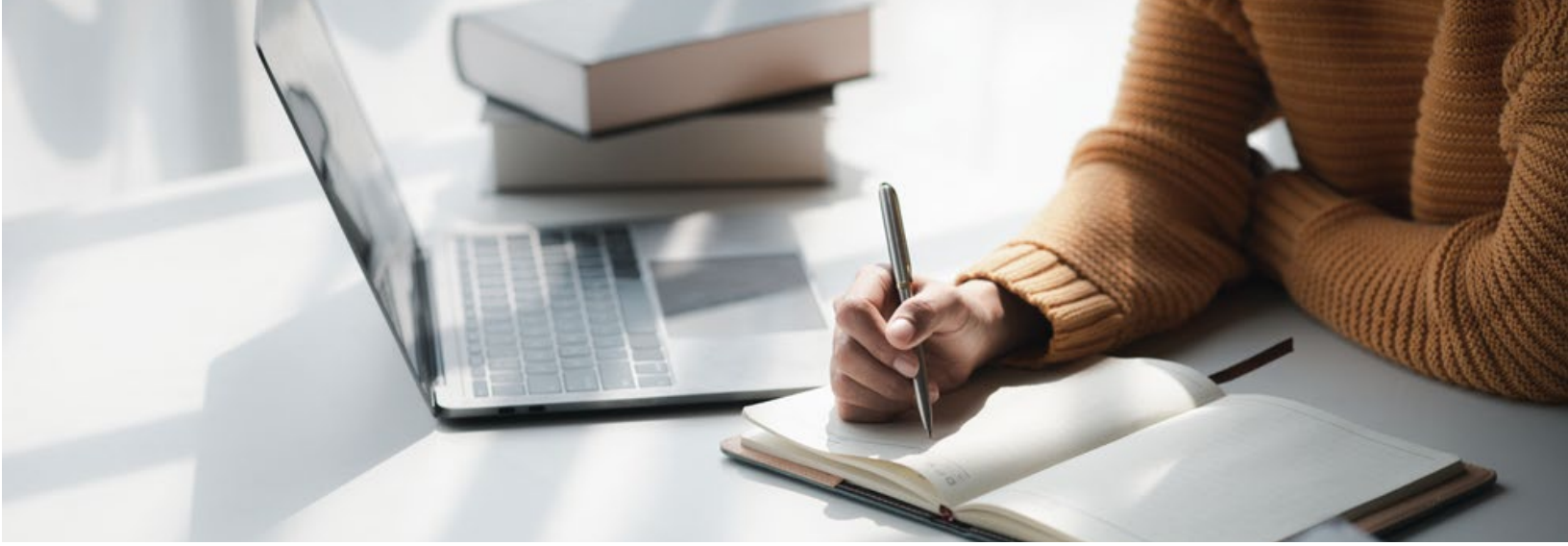
Ejemplo: Un/a usuario publica fotos de sus vacaciones en tiempo real con la ubicación activada, sin darse cuenta de que está compartiendo su localización con desconocidos, lo que representa un riesgo de seguridad.

- **Datos personales y huella digital en redes:** En redes sociales, los datos personales incluyen nombre, correo, número de teléfono, fotos, ubicación y hasta preferencias de contenido. La huella digital es todo lo que dejamos en la web, ya sea por lo que publicamos, damos "me gusta" o buscamos.

Ejemplo: Un/a estudiante completa un test viral en redes que pide datos como su fecha de nacimiento y dirección de correo electrónico. Sin saberlo, está proporcionando información valiosa que podría ser utilizada para publicidad o incluso fraudes.

- **Configuraciones de privacidad en redes sociales:** Cada red social permite ajustar quién puede ver nuestras publicaciones, etiquetarnos en fotos o enviarnos mensajes. Es clave revisar estas opciones para evitar compartir información personal con desconocidos.

Ejemplo: Un/a estudiante recibe solicitudes de amistad de cuentas sospechosas en Facebook. Al revisar su configuración, descubre que su perfil es visible para todos. Ajusta su privacidad para que solo sus amigos puedan ver su información.



Fenómenos negativos que ocurren en redes sociales:

- **Doxxing:** Es la exposición de información personal de una persona en internet sin su consentimiento, con el objetivo de acosarla, amenazarla o perjudicarla. Se obtiene mediante búsquedas en redes sociales, bases de datos públicas o incluso hackeos.

Ejemplo: Un/a estudiante participa en un debate en redes y, tras una discusión, alguien pública su dirección y número de teléfono, lo que lo expone a acoso.

- **Swatting:** Consiste en hacer una denuncia falsa a la policía para que envíen un equipo SWAT o de emergencias a la casa de alguien, haciéndoles creer que hay una situación peligrosa.

Ejemplo: Un/a jugador de videojuegos en línea pierde una partida y, en venganza, otra persona usuaria hace una llamada falsa de amenaza de bomba para que irrumpan en su casa.

- **Catfishing:** Es cuando alguien crea una identidad falsa en redes sociales para engañar a otras personas, generalmente con fines de estafa, acoso o manipulación emocional.

Ejemplo: Un/a adolescente cree estar chateando con una persona de su edad, pero en realidad es un/a persona adulta que se hace pasar por alguien más.

- **Cyberbullying (Ciberacoso):** Acoso, humillación o amenazas a través de internet o redes sociales. Puede incluir comentarios ofensivos, difusión de rumores, insultos, burlas o la publicación de información privada sin permiso.

Ejemplo: Un grupo de estudiantes comparte memes ofensivos sobre un/a compañero en un grupo de WhatsApp, haciéndolo sentir aislado y avergonzado.

- **Sextorsión:** Cuando alguien amenaza con publicar esas imágenes para obtener dinero, favores o más contenido.

Ejemplo: Un/a adolescente envía una foto privada a su pareja, pero luego la imagen se difunde en su escuela sin su permiso.

- **Grooming:** Ocurre cuando una persona adulta se hace pasar por un menor en redes sociales para ganarse la confianza de un/a adolescente o niño/a con intenciones de abuso.

Ejemplo: Un/a niño conoce a alguien en un videojuego en línea que dice tener su edad, pero en realidad es una persona adulta que intenta manipularlo para obtener fotos privadas.

- **Phishing:** Estrategia en la que delincuentes digitales engañan a las personas para que revelen información personal como contraseñas, datos bancarios o accesos a cuentas.

Ejemplo: Un/a estudiante recibe un mensaje falso de Instagram diciendo que su cuenta será eliminada si no verifica su identidad. Ingresa sus datos en un enlace y pierde el acceso a su cuenta.

- **Clickbait y Desinformación:** Clickbait son titulares engañosos que buscan llamar la atención para obtener visitas o reacciones y desinformación son noticias falsas o manipuladas que buscan engañar a la gente con información incorrecta.

Ejemplo: Un post en redes afirma que una nueva ley prohibirá los videojuegos, pero al leer la noticia, resulta ser falso.

Analizando riesgos y protección de la privacidad en redes sociales 15 minutos

Debatir sobre la exposición de datos personales en redes sociales y su impacto en la seguridad digital, respondiendo a las siguientes preguntas:

- ¿Qué riesgos enfrentan las y los niños y adolescentes en redes sociales al compartir fotos privadas?
- ¿Qué medidas pueden prevenir que las y los jóvenes caigan en estas situaciones?
- ¿Qué consecuencias puede tener el ciberacoso en la vida de una persona?
- ¿Qué acciones pueden tomar las y los jóvenes si sufren ciberacoso o se sienten inseguros en línea?
- ¿Qué lección podemos aplicar a nuestra propia vida digital?

Observaciones a las y los docentes:

- *Algunos estudiantes pueden sentirse vulnerables al hablar sobre su experiencia en línea. Es importante crear un ambiente seguro y de respeto donde las y los estudiantes se sientan cómodos compartiendo sus reflexiones.*
- *Promover que las y los estudiantes cuestionen las políticas de privacidad en las plataformas que utilizan, fomentando el pensamiento crítico sobre el control de los datos y su implicación en su vida digital.*

Debatiendo buenas prácticas de privacidad 15 minutos

Leer sobre las configuraciones de privacidad de redes sociales como Facebook, Instagram y TikTok (En caso de que no tengan acceso a internet, llevar impresas las guías de configuración.
A continuación, discutir en grupos pequeños las mejores prácticas para proteger su privacidad en estas plataformas.
Posteriormente, compartir las principales estrategias de seguridad que identifiquen, como:

- No compartir información privada (como fotos, ubicación o datos personales) con desconocidos.
- Configurar las cuentas en redes sociales como privadas.
- Denunciar comportamientos inapropiados o sospechosos en las plataformas digitales.
- Presentar por cada grupo su análisis y las conclusiones que hayan obtenido.

Observaciones a las y los docentes:

- *Asegurarse de que las y los estudiantes dentro de los grupos pequeños participen activamente en la discusión. Puede hacer preguntas guiadas como: "¿Por qué es importante no compartir información personal con desconocidos?" o "¿Cómo se configura tu cuenta para que solo tus amigos puedan ver tus publicaciones?"*
- *Establecer normas claras de respeto durante la discusión, especialmente cuando las y los estudiantes exponen sus ideas. Es importante que el ambiente sea inclusivo para que todos se sientan cómodos compartiendo.*
- *Animar a las y los estudiantes a reflexionar sobre situaciones cotidianas en las que estas buenas prácticas se aplican. Si es posible, use ejemplos reales (de manera general) sobre casos de filtración de datos o riesgos de privacidad en plataformas populares.*

Creando estrategias de protección personal 20 minutos

Crear una Guía de buenas prácticas para proteger la privacidad en redes sociales.
Comenzar realizando una lluvia de ideas y una estructura preliminar, para esto:

- **Individualmente:** Las y los estudiantes escribirán tres ideas clave que consideren esenciales en la guía.
- **En grupos:** compartirán sus ideas y organizan los temas en un esquema lógico.

En esta guía elaborada en Google Docs o en carteleras, deben incluir:

- Configuraciones de privacidad recomendadas en redes sociales populares.
- Consejos para compartir información de forma segura, como el uso de contraseñas fuertes, evitar compartir la ubicación en tiempo real y no aceptar solicitudes de desconocidos.
- Impacto de la inteligencia artificial en la privacidad digital, reflexionando sobre cómo los algoritmos que utilizan diversas redes sociales recopilan datos y cómo protegerse de su explotación.

Observaciones a las y los docentes:

- *Asegurarse de que las y los estudiantes comprendan cómo debe estructurarse la guía (por ejemplo, secciones claras sobre configuraciones de privacidad, consejos de seguridad, y reflexión sobre los algoritmos que usan IA). Esto ayudará a que la creación del documento sea organizada y completa.*
- *Animar a las y los estudiantes a ser creativos en las sugerencias que incluyan, proponiendo medidas prácticas que no sean obvias, como la actualización regular de contraseñas o el uso de autenticación de dos factores.*
- *Durante la elaboración de la guía, sugerirles investigar y usar recursos adicionales sobre privacidad digital, como blogs, artículos, o incluso videos, para enriquecer el contenido de su guía con información actualizada y de diversas fuentes.*

Consolidando 15 minutos

Compartir las mejores recomendaciones de su guía con la clase realizando una exposición oral donde las y los estudiantes expliquen sus recomendaciones.

Observaciones a las y los docentes:

- *Dividir las estrategias en categorías y asignar a cada grupo una categoría diferente. Por ejemplo, un grupo podría enfocarse en configuraciones de privacidad, otro en seguridad de contraseñas, otro en la inteligencia artificial y los datos, etc. Esto garantizará que cada grupo aporte una perspectiva única.*
- *Pedir a las y los estudiantes que incluyan ejemplos concretos en sus recomendaciones para hacerlo más específico. Por ejemplo, en lugar de simplemente decir "no compartir información personal", pueden decir "evitar publicar detalles como tu número de teléfono en una biografía de Instagram".*
- *Asegurarse de que las y los estudiantes tengan acceso al documento colaborativo en línea, como Google Slides, y que cada grupo pueda agregar sus recomendaciones de manera ordenada. Explique cómo colaborar en tiempo real en el documento para maximizar la participación y evitar confusión.*

Sugerencias de evaluación:

Criterios de Evaluación	**Nivel 1** Nivel Inicial	**Nivel 2** Nivel Básico	**Nivel 3** Nivel Avanzado	**Nivel 4** Nivel Experto
Explicación de los aspectos éticos asociados a las soluciones tecnológicas	Identifica de forma muy general que existen riesgos en redes sociales, pero no explica cómo afectan a las personas. No logra relacionarlo con los conceptos trabajados en clase.	Explica de manera básica algunos dilemas éticos en redes sociales, como el impacto de compartir información sin consentimiento. Relaciona su explicación con ejemplos simples vistos en clase.	Analiza con claridad los aspectos éticos en redes sociales, identificando casos como el doxxing o el catfishing. Usa ejemplos del análisis de casos trabajados en la actividad.	Explica con profundidad los riesgos éticos en redes sociales, conectándolos con ejemplos de la actividad de fenómenos negativos en redes y proponiendo formas de actuar con responsabilidad digital.
Explicación de los aspectos sociales asociados a las soluciones tecnológicas	Muestra dificultad para explicar cómo las redes sociales afectan a la sociedad y a la privacidad digital. No identifica conexiones con los fenómenos estudiados.	Describe algunos efectos sociales del uso de redes sociales, como el impacto en la reputación o en la seguridad, pero sin profundizar en su relevancia. Relaciona algunos conceptos de la actividad.	Explica con claridad cómo fenómenos como el cyberbullying o la sextorsión afectan a la sociedad, utilizando ejemplos de los casos analizados en la actividad. Relaciona con el contenido sobre huella digital y datos personales.	Analiza críticamente cómo el uso de redes sociales genera implicaciones sociales a gran escala. Usa ejemplos de la actividad para reflexionar sobre la privacidad digital, la ética y la seguridad en línea. Propone formas de generar conciencia sobre estos temas.
Formulación de medidas de mitigación y descripción del proceso de producción de la solución tecnológica	Propone medidas poco claras o ineficaces para proteger la privacidad en redes sociales. No demuestra comprensión de las herramientas digitales disponibles.	Sugiere algunas estrategias básicas de privacidad, como cambiar configuraciones en redes sociales, pero sin profundizar en su aplicación. Se apoya en la actividad de configuración de privacidad en redes.	Propone medidas concretas y bien explicadas para mejorar la seguridad digital, como la verificación de identidad o el uso de contraseñas seguras. Relaciona su propuesta con los casos analizados en clase.	Diseña estrategias detalladas para mitigar los riesgos en redes sociales. Explica el proceso de implementación de estas soluciones, considerando herramientas digitales y buenas prácticas de seguridad. Usa ejemplos de las configuraciones de privacidad trabajadas en la actividad.

Recursos y sitios web:

- Cápsula alfabetización digital crítica y reflexiva.
- Diplomado Educación híbrida: Módulo 2. Herramientas y aplicaciones para la transición de la educación híbrida.
- "Alerta con los niños: cómo los engañan para que envíen fotos privadas en redes sociales".
- "¿Has sufrido acoso cibernético? Te decimos a dónde acudir".
- Configuraciones de redes sociales: Facebook, Instagram y TikTok.
- Centro de Seguridad de Google.
- Guía para la Protección de la Privacidad en Línea – UNICEF