

Protegiendo nuestro mundo digital: Introducción a la Ingeniería Social

Tecnología e Informática | Informática | para estudiantes de primaria (6-11 años) | 4 semanas

Descripción del Curso

Este curso está diseñado para niños y niñas de 6 a 11 años con el propósito de introducirlos de forma sencilla y segura al concepto de ingeniería social y su relación con la ciberseguridad. A través de actividades divertidas y ejemplos cotidianos, los estudiantes aprenderán cómo proteger su información personal y reconocer cuándo alguien intenta manipularlos para obtener datos o acceso a sus dispositivos.

El curso se dirige a estudiantes de primaria interesados en la tecnología y el uso seguro de internet, promoviendo desde temprana edad hábitos responsables y críticos frente a las interacciones digitales. La metodología es activa, participativa y basada en ejemplos cercanos a la realidad de los niños, combinando explicaciones, juegos, y actividades prácticas que fomentan la reflexión y la prevención.

Al finalizar, los estudiantes serán capaces de identificar situaciones típicas de ingeniería social, comprender la importancia de no compartir información personal con desconocidos, y aplicar estrategias básicas para mantenerse seguros en internet y en el manejo de dispositivos digitales.

Objetivos Generales

- Explicar qué es la ingeniería social y cómo puede afectar la seguridad personal y digital.
- Identificar tipos comunes de solicitudes o mensajes que pueden ser intentos de engaño o manipulación.
- Reconocer qué tipo de información personal no debe compartirse con desconocidos o en internet.
- Aplicar medidas básicas para proteger la información personal y pedir ayuda cuando algo genere duda o incomodidad.
- Valorar la importancia de la seguridad digital y el respeto hacia la privacidad propia y de los demás.

Competencias

- Reconocer situaciones básicas de ingeniería social y posibles intentos de manipulación en entornos digitales y cotidianos.
- Identificar información personal y comprender la importancia de protegerla en internet y en la vida diaria.
- Aplicar medidas sencillas para mantener la seguridad y privacidad en el uso de dispositivos tecnológicos.
- Demostrar habilidades para comunicarse y pedir ayuda ante situaciones de riesgo o dudas sobre seguridad digital.
- Desarrollar una actitud crítica y responsable hacia las interacciones en línea y el uso de la tecnología.

Requerimientos

- Conocimientos básicos sobre el uso de computadoras, tabletas o dispositivos digitales.
- Acceso a internet para actividades supervisadas y recursos multimedia adecuados para niños.
- Materiales para actividades prácticas: papel, colores, hojas para dibujos o diagramas.
- Apoyo y supervisión de un adulto durante las actividades en línea y discusiones.

Unidades del Curso

Unidad 1: ¿Qué es la Ingeniería Social?

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de identificar ejemplos simples de ingeniería social en situaciones cotidianas.
- Al finalizar la unidad, el estudiante será capaz de explicar con sus propias palabras qué es la ingeniería social y cómo puede afectar la seguridad personal.
- Al finalizar la unidad, el estudiante será capaz de distinguir entre solicitudes o mensajes confiables y aquellos que podrían ser intentos de engaño utilizando ejemplos sencillos.
- Al finalizar la unidad, el estudiante será capaz de describir qué tipo de información personal no debe compartirse con desconocidos o en internet.
- Al finalizar la unidad, el estudiante será capaz de expresar la importancia de pedir ayuda a un adulto cuando algo en línea o en persona le cause duda o incomodidad.

Contenidos Temáticos

Introducción a la Ingeniería Social

- ¿Qué es la ingeniería social?
 - Explicación sencilla: personas que intentan engañar para obtener información o acceso.
 - Por qué es importante conocerla para protegernos.
- Ejemplos cotidianos de ingeniería social
 - Situaciones en la escuela, casa o en línea donde alguien puede intentar engañar.
 - Ejemplos simples como pedir una contraseña o hacerse pasar por un amigo.

Cómo identificar intentos de engaño (ingeniería social)

- Señales de alerta en mensajes o solicitudes
 - Solicitudes urgentes o inusuales.
 - Personas desconocidas pidiendo información personal.
- Diferenciar entre mensajes confiables y engañosos

- Ejemplos de mensajes verdaderos y falsos para comparar.
- Preguntar siempre a un adulto cuando algo no se entiende o parece extraño.

Información personal y su protección

- Qué es la información personal
 - Nombre completo, dirección, teléfono, contraseñas, etc.
- Por qué no compartir información personal con desconocidos o en internet
 - Ejemplos de riesgos de compartir datos personales.

La importancia de pedir ayuda

- Cuándo y por qué pedir ayuda a un adulto
 - Si algo en línea o en persona causa duda, miedo o incomodidad.
 - Ejemplos de situaciones que requieren ayuda adulta.
- Cómo comunicar a un adulto lo que pasó

Actividades

Actividad 1: Cuento interactivo sobre engaños

Objetivo: Identificar ejemplos simples de ingeniería social en situaciones cotidianas.

Descripción:

- El docente narra un cuento corto donde un personaje recibe mensajes o preguntas sospechosas.
- En ciertos puntos, se detiene y pregunta a los estudiantes qué harían o si creen que es un engaño.
- Los estudiantes comentan y discuten en grupo las señales que indican que puede ser un intento de engaño.

Organización: grupo completo

Producto esperado: Participación verbal y comprensión del concepto.

Duración estimada: 30 minutos

Actividad 2: Juego de "Verdadero o Falso" con mensajes

Objetivo: Distinguir entre solicitudes o mensajes confiables y aquellos que podrían ser intentos de engaño.

Descripción:

- El docente presenta mensajes escritos simples (en papel o pizarra), algunos confiables y otros con señales de engaño.
- Los estudiantes deben decidir si el mensaje es verdadero o falso y explicar por qué.
- Se discuten las respuestas y se refuerzan las señales de alerta.

Organización: parejas o pequeños grupos

Producto esperado: Lista de mensajes clasificados con justificación.

Duración estimada: 40 minutos

Actividad 3: Mi información personal segura

Objetivo: Describir qué tipo de información personal no debe compartirse con desconocidos o en internet.

Descripción:

- Los estudiantes crean una lista o dibujo con información personal que debe mantenerse privada.
- Se realizan ejemplos de preguntas que no deben contestar sin permiso de un adulto.
- Se comparte con el grupo y se explica la razón de mantener esos datos en secreto.

Organización: individual

Producto esperado: Lista o dibujo con información personal protegida.

Duración estimada: 30 minutos

Actividad 4: Role-play "Pidiendo ayuda a un adulto"

Objetivo: Expresar la importancia de pedir ayuda a un adulto cuando algo cause duda o incomodidad.

Descripción:

- En parejas, los estudiantes representan situaciones donde reciben mensajes o preguntas extrañas.
- Un estudiante actúa como niño que pide ayuda y el otro como adulto que escucha y ayuda.
- Luego se discute la importancia de buscar ayuda y cómo hacerlo.

Organización: parejas

Producto esperado: Representación verbal y reflexión grupal.

Duración estimada: 30 minutos

Evaluación

Evaluación diagnóstica

Qué se evalúa: Conocimientos previos sobre la confianza en mensajes y la información personal.

Cómo se evalúa: Preguntas orales simples al inicio de la unidad, por ejemplo: "¿Qué harías si alguien que no conoces te pide tu nombre?"

Instrumento sugerido: Lista de preguntas orales y observación de respuestas.

Evaluación formativa

Qué se evalúa: Comprensión y aplicación de conceptos durante las actividades (identificación de engaños, mensajes confiables, información personal segura).

Cómo se evalúa: Observación durante actividades, revisión de listas y dibujos, participación en discusiones y role-plays.

Instrumento sugerido: Rúbrica sencilla que valore participación, comprensión y capacidad para explicar conceptos con palabras propias.

Evaluación sumativa

Qué se evalúa: Capacidad para explicar qué es la ingeniería social, identificar ejemplos, distinguir mensajes confiables, proteger información personal y pedir ayuda.

Cómo se evalúa: Ejercicio escrito o verbal donde el estudiante responde preguntas como:

- ¿Qué es la ingeniería social?
- Da un ejemplo de un intento de engaño.
- ¿Qué información no debes compartir?
- ¿Qué harías si algo te hace sentir incómodo en internet?

Instrumento sugerido: Lista de cotejo para respuestas completas y claras.

Unidad 2: Protegiendo nuestra información personal

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de identificar qué datos son personales y cuáles no deben compartirse con desconocidos, tanto en persona como en internet.
- Al finalizar la unidad, el estudiante será capaz de explicar por qué es importante proteger la información personal para evitar riesgos de la ingeniería social.
- Al finalizar la unidad, el estudiante será capaz de distinguir entre situaciones seguras y riesgosas para compartir información personal en diferentes contextos.
- Al finalizar la unidad, el estudiante será capaz de aplicar medidas básicas para proteger su información personal y pedir ayuda cuando algo le genere duda o incomodidad.
- Al finalizar la unidad, el estudiante será capaz de valorar la importancia de respetar la privacidad propia y la de los demás en el entorno digital y presencial.

Contenidos Temáticos

1. ¿Qué es la información personal?

- Definición de información personal: datos que nos identifican y nos hacen únicos.
- Ejemplos de información personal: nombre completo, dirección, número de teléfono, fecha de nacimiento, escuela, contraseñas.
- Diferencia entre datos personales y datos que pueden ser públicos o generales.

2. ¿Por qué es importante proteger nuestra información personal?

- Introducción a la ingeniería social: cómo personas pueden intentar engañarnos para obtener nuestra información.

- Riesgos de compartir información personal con desconocidos: peligros en persona y en internet.
- Consecuencias de no proteger nuestra información: robo de identidad, engaños, pérdida de privacidad.

3. Situaciones seguras y riesgosas para compartir información personal

- Situaciones seguras: compartir con familiares, maestros o adultos de confianza.
- Situaciones riesgosas: compartir con desconocidos en la calle, por teléfono o en internet.
- Ejemplos prácticos para distinguir cuándo y con quién es seguro compartir información.

4. Medidas básicas para proteger la información personal

- No compartir datos personales con desconocidos ni en redes sociales sin permiso.
- Usar contraseñas seguras y no compartirlas.
- Solicitar ayuda a un adulto de confianza cuando algo genera duda o incomodidad.
- Respetar la privacidad propia y la de los demás: no difundir información personal sin permiso.

Actividades

Actividad 1: “Mi caja de datos personales”

Objetivo: Identificar qué datos son personales y cuáles no deben compartirse con desconocidos.

Descripción:

- Se entrega a cada estudiante una hoja con dibujos o recortes de diferentes tipos de datos (nombre, comida favorita, dirección, mascota, etc.).
- Los estudiantes clasifican los datos en dos grupos: “Datos personales que no comparto con desconocidos” y “Datos que puedo compartir”.
- Se discute en grupo para explicar cada decisión.

Organización: Individual y luego discusión grupal.

Producto esperado: Hoja clasificada con datos personales.

Duración estimada: 30 minutos.

Actividad 2: “Historias de cuidado con la información”

Objetivo: Explicar por qué es importante proteger la información para evitar riesgos de ingeniería social.

Descripción:

- El docente narra breves historias o ejemplos donde alguien comparte información personal y luego enfrenta problemas.
- Los estudiantes comentan qué pasó y por qué fue importante proteger esa información.
- En parejas, los estudiantes crean su propia historia de cuidado con la información y la comparten con el grupo.

Organización: Grupal e individual en parejas.

Producto esperado: Historias escritas o contadas que reflejan la importancia de proteger datos personales.

Duración estimada: 40 minutos.

Actividad 3: “Juego de roles: ¿Compartes o no compartes?”

Objetivo: Distinguir entre situaciones seguras y riesgosas para compartir información personal.

Descripción:

- Se presentan diferentes situaciones en tarjetas (ejemplo: un amigo pide tu dirección, un desconocido en línea pide tu nombre completo, un maestro pregunta tu nombre).
- En grupos pequeños, los estudiantes eligen si compartirían o no la información y explican su decisión.
- Se discuten las respuestas con toda la clase.

Organización: Grupos pequeños.

Producto esperado: Listado con decisiones justificadas sobre compartir información.

Duración estimada: 45 minutos.

Actividad 4: “Mi plan para proteger mis datos”

Objetivo: Aplicar medidas básicas para proteger la información personal y pedir ayuda cuando haya dudas.

Descripción:

- Cada estudiante recibe una plantilla para crear su plan personal de protección de datos.
- Incluye acciones como a quién pedir ayuda, qué información no compartir, cómo crear contraseñas seguras.
- Se comparten algunos planes con la clase para reforzar buenas prácticas.

Organización: Individual.

Producto esperado: Plan personal escrito para proteger la información.

Duración estimada: 40 minutos.

Evaluación

Evaluación diagnóstica

Qué se evalúa: Conocimientos previos sobre qué es la información personal y si saben qué datos deben proteger.

Cómo se evalúa: Preguntas orales y una breve actividad de clasificación de datos (datos personales vs. no personales).

Instrumento sugerido: Lista de cotejo simple para observar respuestas y clasificaciones.

Evaluación formativa

Qué se evalúa: Comprensión sobre la importancia de proteger datos, identificación de situaciones seguras o riesgosas, aplicación de medidas básicas.

Cómo se evalúa: Observación durante actividades, participación en juegos de roles y análisis de historias.

Instrumento sugerido: Rúbrica de desempeño con criterios sobre participación, razonamiento y aplicación práctica.

Evaluación sumativa

Qué se evalúa: Capacidad para identificar datos personales, explicar la importancia de protegerlos, distinguir situaciones seguras y riesgosas, y presentar un plan de protección personal.

Cómo se evalúa: Evaluación escrita y presentación oral del plan personal para proteger la información.

Instrumento sugerido: Prueba corta con preguntas de opción múltiple y respuestas abiertas, además de una rúbrica para evaluar el plan personal.

Unidad 3: Reconociendo intentos de engaño

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de identificar mensajes o correos electrónicos sospechosos que podrían ser intentos de engaño, usando ejemplos vistos en clase.
- Al finalizar la unidad, el estudiante será capaz de describir señales comunes de manipulación en mensajes, como solicitudes urgentes o promesas falsas, en actividades de análisis de textos.
- Al finalizar la unidad, el estudiante será capaz de diferenciar entre mensajes seguros y mensajes potencialmente peligrosos mediante ejercicios prácticos con situaciones simuladas.
- Al finalizar la unidad, el estudiante será capaz de explicar por qué no debe compartir información personal ante solicitudes desconocidas, apoyándose en casos ilustrativos presentados durante la unidad.
- Al finalizar la unidad, el estudiante será capaz de aplicar estrategias básicas para pedir ayuda a un adulto cuando reciba un mensaje o situación que le genere duda o incomodidad, en role plays guiados.

Contenidos Temáticos

1. Introducción a los mensajes y correos sospechosos

- ¿Qué es un mensaje o correo sospechoso?
 - Explicación sencilla de mensajes que buscan engañar o manipular.
- Ejemplos comunes de mensajes engañosos para niños
 - Presentación de ejemplos simples y adaptados, como mensajes que ofrecen regalos o piden información personal.

2. Señales comunes de manipulación en mensajes

- Solicitudes urgentes o de presión
 - ¿Por qué nos piden hacer algo rápido?
- Promesas falsas o regalos que parecen demasiado buenos para ser verdad

- Cómo identificar ofertas engañosas.
- Errores o mensajes extraños en el texto
 - Ortografía, gramática y frases raras como señales de alerta.

3. Diferenciando mensajes seguros de peligrosos

- Características de un mensaje seguro
 - Quién envía el mensaje y cómo lo hace.
- Ejercicios con mensajes simulados para identificar riesgos
- Uso de preguntas para pensar antes de confiar en un mensaje

4. Protección de la información personal

- Por qué no compartir datos personales con desconocidos
 - Ejemplos de consecuencias de compartir información.
- Qué información es personal y debe protegerse

5. Estrategias para pedir ayuda a un adulto

- Cuándo y cómo pedir ayuda a alguien de confianza
- Role plays y prácticas para expresar dudas o incomodidad
- Reconocer señales internas que indican que se debe pedir ayuda

Actividades

Actividad 1: "Detectives de mensajes sospechosos"

Objetivo: Identificar mensajes o correos electrónicos sospechosos usando ejemplos vistos en clase.

Descripción:

- El docente presenta varios ejemplos de mensajes (impresos o en pantalla), algunos seguros y otros sospechosos.
- Los estudiantes, en parejas, analizan cada mensaje y marcan si les parece seguro o sospechoso, justificando su elección con palabras o dibujos.
- Se realiza una puesta en común para discutir las respuestas y aclarar dudas.

Organización: Parejas

Producto esperado: Listado o cartel con mensajes clasificados y razones de su clasificación.

Duración estimada: 45 minutos

Actividad 2: "Señales de alerta en mensajes"

Objetivo: Describir señales comunes de manipulación en mensajes mediante análisis de textos.

Descripción:

- El docente entrega textos cortos con mensajes que contienen señales de manipulación (urgencia, promesas falsas, errores).
- Individualmente, los estudiantes subrayan o rodean las palabras o frases que les parecen señales de alerta.
- Luego, en grupo pequeño, comparten sus hallazgos y el docente refuerza los conceptos.

Organización: Individual y luego grupos pequeños

Producto esperado: Textos marcados con señales identificadas y explicación oral o escrita.

Duración estimada: 40 minutos

Actividad 3: "¿Mensaje seguro o peligroso?" - Simulación práctica

Objetivo: Diferenciar entre mensajes seguros y potencialmente peligrosos mediante ejercicios prácticos.

Descripción:

- Se reparte a cada grupo un conjunto de tarjetas con mensajes simulados.
- Los estudiantes leen en voz alta cada mensaje y colocan la tarjeta en dos cajas: "Seguro" o "Peligroso".
- El docente guía la discusión sobre por qué cada mensaje es seguro o no, reforzando criterios.

Organización: Grupos pequeños

Producto esperado: Clasificación correcta de tarjetas y argumentos para su clasificación.

Duración estimada: 50 minutos

Actividad 4: "¿Qué harías tú?" - Role play para pedir ayuda

Objetivo: Aplicar estrategias básicas para pedir ayuda a un adulto ante mensajes o situaciones dudosas.

Descripción:

- El docente presenta escenarios breves donde un niño recibe un mensaje extraño o incómodo.
- Por parejas, los estudiantes representan la situación y practican cómo pedir ayuda a un adulto.
- Se realiza una reflexión grupal sobre la importancia de pedir ayuda y cómo hacerlo.

Organización: Parejas y toda la clase para reflexión

Producto esperado: Presentaciones de role plays y conclusiones escritas o orales sobre pedir ayuda.

Duración estimada: 45 minutos

Evaluación

Evaluación diagnóstica

Qué se evalúa: Conocimientos previos sobre mensajes sospechosos y seguridad digital.

Cómo se evalúa: Mediante preguntas orales y un breve juego de clasificación de mensajes al inicio de la unidad.

Instrumento sugerido: Cuestionario sencillo con ejemplos visuales y preguntas abiertas.

Evaluación formativa

Qué se evalúa: Identificación de señales de manipulación, capacidad de análisis de mensajes, y habilidades para pedir ayuda.

Cómo se evalúa: Observación durante actividades, revisión de trabajos escritos, y participación en role plays.

Instrumento sugerido: Lista de cotejo para observar participación y respuestas, revisión de textos marcados y autoevaluación guiada.

Evaluación sumativa

Qué se evalúa: Capacidad para identificar mensajes sospechosos, describir señales de manipulación, diferenciar mensajes, explicar la protección de información personal y demostrar cómo pedir ayuda.

Cómo se evalúa: Prueba práctica con mensajes reales y simulados a analizar, un breve cuestionario escrito y presentación de un role play final.

Instrumento sugerido: Rúbrica para evaluar análisis de mensajes y role plays, prueba escrita adaptada con imágenes y preguntas sencillas.

Unidad 4: Estrategias para mantenernos seguros

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de identificar situaciones en las que debe pedir ayuda a un adulto cuando algo en línea le cause duda o incomodidad.
- Al finalizar la unidad, el estudiante será capaz de explicar por qué no debe compartir contraseñas ni información personal con desconocidos o en internet.
- Al finalizar la unidad, el estudiante será capaz de demostrar hábitos seguros al pensar antes de responder mensajes o hacer clic en enlaces sospechosos.
- Al finalizar la unidad, el estudiante será capaz de aplicar al menos tres acciones prácticas para proteger su seguridad personal y digital en situaciones cotidianas.

Contenidos Temáticos

1. Reconociendo cuándo pedir ayuda a un adulto

- **¿Qué es una situación que nos hace sentir incómodos en línea?**

Se explicará con ejemplos sencillos cómo identificar mensajes, imágenes o solicitudes que causen duda o incomodidad.

- **¿Quiénes son los adultos confiables?**

Se hablará sobre quiénes pueden ayudar: padres, maestros, familiares u otros adultos responsables.

- **Cómo pedir ayuda de manera segura**

Se enseñará a comunicar lo que pasó sin miedo ni vergüenza, y la importancia de hacerlo pronto.

2. La importancia de no compartir contraseñas ni información personal

- **¿Qué son las contraseñas y para qué sirven?**

Definición básica y ejemplos de contraseñas que usamos.

- **Por qué no debemos compartir contraseñas con nadie**

Se explicará que las contraseñas son “secretos” para protegernos y que compartirlas puede causar problemas.

- **Qué información personal no se debe compartir en internet**

Ejemplos: dirección, número de teléfono, escuela, fotos personales.

3. Hábitos seguros en la comunicación digital

- **¿Qué es pensar antes de responder?**

Se fomentará la pausa para reflexionar antes de contestar mensajes o correos.

- **¿Por qué no debemos hacer clic en enlaces sospechosos?**

Se explicará que algunos enlaces pueden contener virus o engaños.

- **Cómo reconocer mensajes o enlaces sospechosos**

Se mostrarán características comunes de mensajes falsos o peligrosos.

4. Acciones prácticas para proteger nuestra seguridad personal y digital

- **Crear contraseñas seguras y guardarlas bien**

Ejemplos de contraseñas fáciles de recordar pero seguras.

- **Configurar la privacidad en juegos y aplicaciones**

Se enseñará la importancia de ajustar la privacidad para evitar compartir información con desconocidos.

- **Practicar el hábito de consultar con un adulto antes de hacer algo dudoso**

Ejemplos prácticos para aplicar en la vida diaria.

Actividades

Actividad 1: "Dibuja y cuenta cuándo pedir ayuda"

Objetivo: Identificar situaciones en las que se debe pedir ayuda a un adulto.

Descripción:

- El docente presenta situaciones ficticias con imágenes y relatos sencillos.
- Los estudiantes dibujan una situación en la que se sentirían incómodos en línea y luego explican a la clase qué harían y a quién pedirían ayuda.
- Se discute en grupo para reforzar la importancia de pedir ayuda.

Organización: Individual

Producto esperado: Dibujo con explicación oral o escrita breve.

Duración: 40 minutos

Actividad 2: "Juego de roles: No comparto mi contraseña"

Objetivo: Explicar por qué no compartir contraseñas ni información personal.

Descripción:

- Se forman parejas donde un estudiante actúa como alguien que pide información personal o contraseñas, y el otro responde con razones y estrategias para no compartirla.
- Luego alternan roles.
- Al final, cada pareja comparte con el grupo algunas frases o razones para proteger sus contraseñas.

Organización: Parejas

Producto esperado: Diálogo actuado y lista de frases para proteger información.

Duración: 45 minutos

Actividad 3: "Detectives de mensajes sospechosos"

Objetivo: Demostrar hábitos seguros al pensar antes de responder y reconocer mensajes o enlaces sospechosos.

Descripción:

- El docente entrega ejemplos de mensajes o correos electrónicos (reales o ficticios) que pueden ser seguros o sospechosos.
- Los estudiantes, en grupos, analizan cada mensaje y deciden si es seguro o no, justificando su respuesta.
- Proponen qué acciones tomarían (no responder, pedir ayuda, borrar el mensaje, etc.).

Organización: Grupos pequeños

Producto esperado: Lista de mensajes analizados con decisiones y justificaciones.

Duración: 50 minutos

Actividad 4: "Mi plan de seguridad digital"

Objetivo: Aplicar al menos tres acciones prácticas para proteger su seguridad personal y digital.

Descripción:

- Cada estudiante recibe una plantilla para escribir o dibujar tres acciones que realizará para estar seguro en internet.
- Puede incluir: pedir ayuda, no compartir contraseñas, pensar antes de hacer clic, entre otras.
- Se comparten los planes con el grupo y se acuerda revisarlos en el futuro para ver cómo van aplicándolos.

Organización: Individual

Producto esperado: Plan personal de seguridad digital.

Duración: 40 minutos

Evaluación

Evaluación diagnóstica

Qué se evalúa: Conocimientos previos sobre pedir ayuda, compartir información y hábitos en internet.

Cómo se evalúa: Preguntas orales y discusión grupal al inicio de la unidad para conocer las ideas y experiencias de los estudiantes.

Instrumento sugerido: Lista de preguntas guía para el docente y registro anecdótico.

Evaluación formativa

Qué se evalúa: Progreso en la identificación de situaciones de riesgo, comprensión de la importancia de la privacidad y aplicación de hábitos seguros.

Cómo se evalúa: Observación durante actividades prácticas, revisión de dibujos, dramatizaciones y análisis de mensajes, retroalimentación continua.

Instrumento sugerido: Rúbrica sencilla para evaluar participación, comprensión y aplicación en actividades.

Evaluación sumativa

Qué se evalúa: Capacidad para identificar situaciones para pedir ayuda, explicar por qué no compartir contraseñas, demostrar hábitos seguros y aplicar acciones prácticas.

Cómo se evalúa: Presentación del plan personal de seguridad digital y respuestas a un cuestionario corto con preguntas relacionadas a los objetivos.

Instrumento sugerido: Cuestionario de opción múltiple y/o preguntas abiertas adaptadas al nivel, y evaluación del plan personal con lista de cotejo.