

Seguridad en Redes Sociales: Protege tu Identidad Digital

Tecnología e Informática | Manejo de Información | para estudiantes de secundaria (12-15 años) | 4 semanas

Descripción del Curso

Este curso está diseñado para estudiantes de secundaria interesados en aprender a navegar y utilizar las redes sociales de forma segura y responsable. A lo largo de cuatro semanas, los alumnos explorarán los principales riesgos y buenas prácticas para proteger su información personal y su privacidad en línea. Se enfatiza el desarrollo de habilidades críticas para identificar amenazas, configurar adecuadamente la privacidad y adoptar un comportamiento digital seguro.

Dirigido a jóvenes de 12 a 15 años, el curso utiliza un enfoque metodológico participativo con actividades prácticas, análisis de casos reales y discusiones grupales que facilitan la comprensión y aplicación de conceptos. Al finalizar, los estudiantes estarán capacitados para gestionar sus perfiles en redes sociales con mayor responsabilidad y tomar decisiones informadas que resguarden su seguridad digital, contribuyendo a un entorno virtual más seguro para ellos y su comunidad.

Objetivos Generales

- Analizar los riesgos asociados al uso de redes sociales y su impacto en la seguridad personal.
- Aplicar configuraciones de privacidad y seguridad en diferentes plataformas sociales.
- Evaluar situaciones de riesgo digital y adoptar estrategias para prevenir y actuar frente a ellas.
- Comunicar de forma efectiva y segura en entornos digitales fomentando el respeto y la responsabilidad.

Competencias

- Identificar diferentes tipos de riesgos y amenazas comunes en redes sociales.
- Configurar adecuadamente la privacidad y seguridad en distintas plataformas sociales.
- Aplicar buenas prácticas para proteger la información personal en entornos digitales.
- Reconocer y responder adecuadamente a situaciones de ciberacoso y engaños en línea.
- Desarrollar una actitud crítica y responsable frente al uso de redes sociales.

Requerimientos

- Conocimientos básicos sobre el uso de dispositivos digitales (computadora, teléfono móvil).
- Acceso a una computadora o dispositivo con conexión a internet.
- Cuenta básica en alguna red social para prácticas (opcional, pero recomendado).
- Material de apoyo proporcionado por el docente (guías, videos, casos de estudio).

Unidades del Curso

Unidad 1: Introducción a las Redes Sociales y su Seguridad

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de identificar los conceptos básicos de las redes sociales y su función en la comunicación cotidiana.
- Al finalizar la unidad, el estudiante será capaz de describir la importancia de las redes sociales en la vida personal y social, reconociendo su impacto positivo y negativo.
- Al finalizar la unidad, el estudiante será capaz de enumerar los riesgos generales asociados al uso de redes sociales, incluyendo amenazas a la seguridad y la privacidad.
- Al finalizar la unidad, el estudiante será capaz de explicar las principales medidas de seguridad y privacidad que se deben considerar al utilizar redes sociales.
- Al finalizar la unidad, el estudiante será capaz de analizar ejemplos de situaciones de riesgo en redes sociales para identificar posibles consecuencias y la necesidad de precaución.

Contenidos Temáticos

1. Conceptos básicos de las redes sociales

- **Definición de redes sociales:** Se explicará qué son las redes sociales, destacando su naturaleza como plataformas digitales que permiten la interacción, comunicación y creación de comunidades en línea.
- **Tipos de redes sociales más comunes:** Se presentarán ejemplos populares (Facebook, Instagram, TikTok, Twitter, WhatsApp) y su función principal.
- **Elementos fundamentales de una red social:** Perfiles, amigos/contactos, publicaciones, mensajes, y grupos/comunidades.
- **Funciones de las redes sociales en la comunicación cotidiana:** Cómo se usan para compartir información, mantenerse en contacto, expresar opiniones y organizar eventos.

2. Importancia y impacto de las redes sociales en la vida personal y social

- **Impacto positivo:** Facilitan la comunicación, el aprendizaje colaborativo, la construcción de identidad y el acceso a información.
- **Impacto negativo:** Posibilidad de distracción, dependencia, presión social, y exposición a contenidos inapropiados o dañinos.
- **Ejemplos de usos responsables y beneficiosos:** Uso para proyectos escolares, mantenerse en contacto con familiares, promover causas sociales.
- **Reflexión sobre el equilibrio en el uso:** La importancia de usar las redes sociales de manera consciente y equilibrada.

3. Riesgos generales en el uso de redes sociales

- **Riesgos a la seguridad:** Suplantación de identidad, virus o software malicioso, fraudes y estafas.
- **Riesgos a la privacidad:** Exposición de datos personales, geo-localización, acceso no autorizado a información privada.
- **Riesgos sociales y emocionales:** Ciberacoso, sexting, presión grupal, fake news (noticias falsas).
- **Consecuencias potenciales:** Daño a la reputación, problemas legales, impacto en la salud mental.

4. Medidas básicas de seguridad y privacidad en redes sociales

- **Configuración de privacidad:** Cómo ajustar la visibilidad de la información personal y publicaciones.
- **Contraseñas seguras:** Características de una contraseña fuerte y la importancia de no compartirla.
- **Reconocimiento y manejo de solicitudes sospechosas:** Evitar aceptar solicitudes o mensajes de desconocidos.
- **Uso responsable de la información personal:** Qué datos no compartir y por qué.
- **Actualizaciones y uso de antivirus:** Mantener el software actualizado para evitar vulnerabilidades.

5. Análisis de situaciones de riesgo en redes sociales

- **Estudio de casos reales o hipotéticos:** Ejemplos de situaciones de riesgo como el ciberacoso o divulgación de información personal.
- **Identificación de señales de alerta:** Reconocer comportamientos o mensajes sospechosos.
- **Discusión de consecuencias:** Impacto personal, social y legal de las situaciones analizadas.
- **Estrategias para actuar con precaución y protegerse:** Pasos a seguir ante situaciones de riesgo.

Actividades

Actividad 1: Mapa conceptual de redes sociales

Objetivo: Identificar los conceptos básicos de las redes sociales y su función en la comunicación cotidiana.

Descripción:

- El docente presenta una breve explicación introductoria sobre qué son las redes sociales.
- Los estudiantes, en parejas, crean un mapa conceptual que incluya definición, tipos de redes sociales y funciones principales.
- Usan papel o herramientas digitales sencillas (como Canva o MindMeister).
- Comparten y explican su mapa al grupo, fomentando la retroalimentación.

Organización: Parejas

Producto esperado: Mapa conceptual claro y organizado sobre redes sociales.

Duración estimada: 45 minutos

Actividad 2: Debate sobre el impacto de las redes sociales

Objetivo: Describir la importancia de las redes sociales en la vida personal y social, reconociendo su impacto positivo y negativo.

Descripción:

- Dividir a la clase en dos grupos: uno defenderá los aspectos positivos y otro los negativos de las redes sociales.
- Cada grupo prepara argumentos basados en ejemplos cotidianos y experiencias propias.
- Se realiza el debate moderado por el docente.
- Al final, se reflexiona sobre la necesidad de un uso equilibrado.

Organización: Grupos

Producto esperado: Participación activa en debate y reflexión escrita breve individual sobre el equilibrio en el uso.

Duración estimada: 60 minutos

Actividad 3: Taller de identificación de riesgos y medidas de seguridad

Objetivo: Enumerar los riesgos generales asociados al uso de redes sociales y explicar las principales medidas de seguridad y privacidad.

Descripción:

- El docente presenta diversos riesgos mediante imágenes, videos o relatos breves.
- En grupos pequeños, los estudiantes listan los riesgos que identifican y proponen medidas para prevenirlos.
- Se realiza una puesta en común donde el docente complementa con medidas clave.
- Se entrega un folleto o ficha con recomendaciones para uso seguro.

Organización: Grupos pequeños

Producto esperado: Listado de riesgos y medidas de seguridad, y ficha informativa.

Duración estimada: 50 minutos

Actividad 4: Análisis de casos de riesgo en redes sociales

Objetivo: Analizar ejemplos de situaciones de riesgo para identificar posibles consecuencias y la necesidad de precaución.

Descripción:

- Se presentan casos hipotéticos escritos o en video donde se muestran situaciones de riesgo (ciberacoso, suplantación, exposición de información).
- Los estudiantes, en parejas o tríos, analizan el caso respondiendo preguntas guiadas: ¿Qué riesgos hay? ¿Qué consecuencias pueden ocurrir? ¿Qué medidas se podrían tomar?
- Se comparte el análisis con el grupo y se reflexiona sobre la importancia de actuar con precaución.

Organización: Parejas o tríos

Producto esperado: Informe breve con análisis de riesgos y medidas preventivas.

Duración estimada: 60 minutos

Evaluación

Evaluación diagnóstica

Qué se evalúa: Conocimientos previos sobre qué son las redes sociales y usos que les dan los estudiantes.

Cómo se evalúa: Mediante una lluvia de ideas y preguntas orales al inicio de la unidad para conocer nociones y experiencias previas.

Instrumento sugerido: Registro anecdótico del docente o esquema simple en pizarra.

Evaluación formativa

Qué se evalúa: Comprensión de conceptos, identificación de riesgos y aplicación de medidas de seguridad durante las actividades.

Cómo se evalúa: Observación directa durante actividades, revisión de productos (mapas conceptuales, listas, análisis de casos) y participación en debates.

Instrumento sugerido: Rúbrica de desempeño que valore claridad, pertinencia y participación.

Evaluación sumativa

Qué se evalúa: Dominio integral de los conceptos básicos, importancia, riesgos, medidas de seguridad y análisis crítico de situaciones de riesgo.

Cómo se evalúa: Prueba escrita con preguntas de opción múltiple, preguntas abiertas para describir riesgos y medidas, y un caso para analizar y responder.

Instrumento sugerido: Examen diseñado con preguntas alineadas a los objetivos, con criterios claros de corrección.

Unidad 2: Riesgos Comunes y Amenazas en Redes Sociales

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de identificar diferentes tipos de amenazas digitales como el ciberacoso, phishing y suplantación de identidad mediante la revisión de casos prácticos.
- Al finalizar la unidad, el estudiante será capaz de describir las características y consecuencias de los riesgos comunes en redes sociales utilizando ejemplos reales o simulados.
- Al finalizar la unidad, el estudiante será capaz de analizar situaciones de riesgo digital presentadas en escenarios para determinar el nivel de amenaza y posibles impactos en la seguridad personal.
- Al finalizar la unidad, el estudiante será capaz de proponer estrategias básicas para prevenir y actuar frente a amenazas digitales, aplicando medidas de seguridad aprendidas en clase.
- Al finalizar la unidad, el estudiante será capaz de comunicar de manera clara y respetuosa la importancia de reconocer y responder a los riesgos en redes sociales mediante debates o presentaciones grupales.

Contenidos Temáticos

1. Introducción a los riesgos en redes sociales

- Definición de riesgos y amenazas digitales: explicación sencilla de qué son los riesgos y por qué son importantes.
- Importancia de la seguridad en redes sociales: impacto de una mala gestión de la seguridad en la vida cotidiana y personal.

2. Tipos comunes de amenazas en redes sociales

- Ciberacoso (Cyberbullying):
 - Descripción y ejemplos: qué es, cómo se manifiesta.
 - Impactos emocionales y sociales en las víctimas.
- Phishing:
 - Definición y técnicas comunes: correos, mensajes y enlaces falsos.
 - Cómo reconocer intentos de phishing.
- Suplantación de identidad (Impersonation):
 - Qué es y cómo se realiza.
 - Consecuencias para la persona afectada.
- Otros riesgos frecuentes:
 - Malware y virus a través de links.
 - Exposición de información personal sensible.
 - Estafas y fraudes en redes sociales.

3. Análisis de casos prácticos de amenazas digitales

- Presentación de casos reales o simulados: historias breves sobre ciberacoso, phishing y suplantación.
- Identificación de señales de alerta en cada caso.
- Discusión sobre posibles consecuencias y niveles de amenaza.

4. Estrategias para prevenir y actuar frente a amenazas en redes sociales

- Medidas básicas de seguridad:
 - Configuración de privacidad en perfiles.
 - Reconocimiento y bloqueo de usuarios sospechosos.
 - Uso de contraseñas seguras y autenticación en dos pasos.
- Qué hacer si se es víctima o testigo de una amenaza digital:
 - Pasos para reportar contenido o usuarios.
 - Apoyo a víctimas y comunicación con adultos responsables.
- Promoción de comportamientos respetuosos y responsables en línea.

5. Comunicación y sensibilización sobre riesgos digitales

- Importancia de hablar sobre seguridad digital con respeto y claridad.
- Técnicas para presentar información y debatir sobre riesgos y prevención.
- El rol de cada estudiante en la construcción de un entorno digital seguro.

Actividades

Actividad 1: Identificación de amenazas mediante casos prácticos

Objetivo: Identificar diferentes tipos de amenazas digitales como el ciberacoso, phishing y suplantación de identidad mediante la revisión de casos prácticos.

Descripción:

- El docente presenta 3-4 casos breves (reales o simulados) que involucran distintas amenazas en redes sociales.
- En parejas, los estudiantes leen cada caso y discuten cuál es la amenaza digital que se presenta.
- Luego, clasifican cada caso según el tipo de riesgo y enumeran señales de alerta que detectaron.
- Finalmente, comparten sus conclusiones con el grupo para retroalimentación.

Organización: Parejas

Producto esperado: Listado clasificado de casos con la amenaza identificada y señales de alerta.

Duración estimada: 50 minutos

Actividad 2: Mapa mental de riesgos y consecuencias

Objetivo: Describir las características y consecuencias de los riesgos comunes en redes sociales utilizando ejemplos reales o simulados.

Descripción:

- En grupos de 3-4 estudiantes, elaboran un mapa mental que incluya los tipos de amenazas, sus características y posibles consecuencias para la persona afectada.
- Utilizan ejemplos vistos en clase o investigados previamente para ilustrar cada riesgo.
- Preparan una breve explicación oral para presentar su mapa al resto de la clase.

Organización: Grupos pequeños

Producto esperado: Mapa mental digital o en papel y presentación oral breve.

Duración estimada: 1 hora

Actividad 3: Análisis de escenarios y propuestas de prevención

Objetivo: Analizar situaciones de riesgo digital para determinar nivel de amenaza y proponer estrategias para prevenir y actuar.

Descripción:

- El docente presenta varios escenarios simulados con diferentes niveles de riesgo en redes sociales.

- Individualmente, los estudiantes analizan cada escenario, identifican el nivel de amenaza (bajo, medio, alto) y describen los posibles impactos.
- Luego, proponen al menos dos estrategias o medidas para prevenir o responder adecuadamente a la amenaza.
- Se realiza una puesta en común para discutir las propuestas y aclarar dudas.

Organización: Individual y luego grupo grande

Producto esperado: Fichas de análisis con nivel de amenaza, impactos y estrategias.

Duración estimada: 1 hora 15 minutos

Actividad 4: Debate grupal sobre la importancia de la seguridad en redes sociales

Objetivo: Comunicar de manera clara y respetuosa la importancia de reconocer y responder a los riesgos en redes sociales.

Descripción:

- Dividir la clase en dos grupos: uno a favor de la importancia de la prevención activa y otro que discuta los desafíos para lograrla.
- Cada grupo prepara argumentos basados en lo aprendido y experiencias personales o casos estudiados.
- Se realiza un debate guiado por el docente, promoviendo respeto y escucha activa.
- Al finalizar, cada estudiante escribe una reflexión breve sobre la importancia de la seguridad digital.

Organización: Grupos y luego individual

Producto esperado: Participación en debate y reflexión escrita individual.

Duración estimada: 50 minutos

Evaluación

Evaluación diagnóstica

Qué se evalúa: Conocimientos previos sobre tipos de amenazas digitales y experiencias personales con riesgos en redes sociales.

Cómo se evalúa: Cuestionario corto con preguntas abiertas y de opción múltiple al inicio de la unidad.

Instrumento sugerido: Test en papel o digital con 8-10 preguntas simples.

Evaluación formativa

Qué se evalúa: Progreso en la identificación de riesgos, análisis de casos y aplicación de estrategias preventivas.

Cómo se evalúa: Observación durante actividades grupales e individuales, revisión de productos parciales (mapas mentales, fichas de análisis) y participación en debates.

Instrumento sugerido: Rúbrica de desempeño que contemple criterios como claridad, precisión, colaboración y argumentación.

Evaluación sumativa

Qué se evalúa: Capacidad integral para identificar amenazas, describir características y consecuencias, analizar situaciones de riesgo, proponer estrategias preventivas y comunicar la importancia de la seguridad.

Cómo se evalúa: Trabajo final que incluya un análisis escrito de un caso real o simulado, con propuestas de prevención y una presentación oral o digital para compartir con el grupo.

Instrumento sugerido: Rúbrica de evaluación del trabajo final que valore contenido, análisis crítico, propuestas y habilidades comunicativas.

Unidad 3: Configuración de Privacidad y Seguridad en Redes Sociales

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de identificar las diferentes opciones de configuración de privacidad en plataformas sociales comunes mediante la exploración guiada de sus menús.
- Al finalizar la unidad, el estudiante será capaz de ajustar las configuraciones de privacidad para limitar el acceso a su información personal en al menos dos redes sociales, siguiendo pasos específicos y verificados.
- Al finalizar la unidad, el estudiante será capaz de evaluar y comparar configuraciones predeterminadas de privacidad en diferentes redes sociales para determinar cuáles protegen mejor su identidad digital.
- Al finalizar la unidad, el estudiante será capaz de crear una guía sencilla para configurar la privacidad y seguridad en una red social elegida, explicando la importancia de cada ajuste para proteger su información personal.

Contenidos Temáticos

1. Introducción a la privacidad y seguridad en redes sociales

- ¿Qué es la privacidad digital?
Concepto básico de privacidad en internet y su importancia en redes sociales.
- Riesgos de no proteger la información personal
Ejemplos de problemas por exposición de datos personales: robo de identidad, acoso, spam.

2. Exploración de opciones de configuración de privacidad en redes sociales comunes

- Principales redes sociales estudiadas: Facebook, Instagram, TikTok, WhatsApp
Descripción breve de cada plataforma y su popularidad.
- Menús y secciones de configuración de privacidad
Localización y navegación por las opciones de privacidad en cada red social.
- Tipos de configuraciones: quién puede ver publicaciones, quién puede contactar, control de etiquetas, historial de actividad

3. Ajuste de configuraciones de privacidad para proteger la información personal

- Pasos detallados para modificar configuraciones en Facebook
Cómo limitar audiencia de publicaciones, bloquear usuarios, controlar visibilidad de información personal.
- Pasos detallados para modificar configuraciones en Instagram
Configuración de cuenta privada, control de comentarios, gestión de seguidores.
- Configuraciones recomendadas para garantizar privacidad y seguridad
Configuraciones predeterminadas vs configuraciones personalizadas para mayor seguridad.

4. Evaluación y comparación de configuraciones predeterminadas de privacidad entre redes sociales

- Definición de configuraciones predeterminadas
Qué son y por qué importan.
- Comparativa entre redes sociales sobre privacidad predeterminada
Ventajas y desventajas de la configuración inicial de cada plataforma.
- Criterios para evaluar qué tan segura es una configuración predeterminada
Accesibilidad, control del usuario, nivel de exposición de datos.

5. Creación de una guía sencilla para configurar privacidad y seguridad en una red social

- Pasos para redactar una guía clara y sencilla
Uso de lenguaje accesible, ilustraciones o capturas de pantalla.
- Explicación de la importancia de cada ajuste
Qué protege y por qué es importante modificarlo.
- Presentación y revisión de la guía con compañeros
Retroalimentación para mejorar claridad y precisión.

Actividades

Actividad 1: Exploración guiada de menús de configuración de privacidad

Objetivo: Identificar las diferentes opciones de configuración de privacidad en plataformas sociales comunes.

Descripción:

- El docente presenta una breve explicación sobre privacidad en redes sociales.
- Los estudiantes acceden a Facebook e Instagram (o redes disponibles) desde sus dispositivos.
- Siguiendo una guía paso a paso, exploran los menús de configuración de privacidad y anotan las opciones que encuentran.
- Discuten en plenaria las diferencias y semejanzas encontradas en cada plataforma.

Organización: Individual

Producto esperado: Lista anotada con las opciones de privacidad encontradas en cada red social explorada.

Duración: 60 minutos

Actividad 2: Ajuste práctico de configuraciones de privacidad en dos redes sociales

Objetivo: Ajustar configuraciones para limitar el acceso a información personal en al menos dos redes sociales.

Descripción:

- El docente entrega un instructivo detallado con pasos para modificar configuraciones en Facebook e Instagram.
- Los estudiantes siguen los pasos para configurar su propia cuenta o una cuenta de práctica, ajustando la privacidad según recomendaciones.
- Realizan capturas de pantalla o anotan los cambios realizados.
- Comparten en parejas los ajustes realizados y explican las razones de cada cambio.

Organización: Individual y parejas (para discusión)

Producto esperado: Registro de configuraciones modificadas (capturas o anotaciones) y explicación oral de los ajustes.

Duración: 90 minutos

Actividad 3: Análisis comparativo de configuraciones predeterminadas de privacidad

Objetivo: Evaluar y comparar configuraciones predeterminadas para determinar cuál protege mejor la identidad digital.

Descripción:

- En grupos, los estudiantes investigan las configuraciones predeterminadas de privacidad en Facebook, Instagram y TikTok.
- Crean una tabla comparativa con ventajas, desventajas y nivel de protección de cada configuración inicial.
- Presentan sus conclusiones al grupo y discuten cuál plataforma ofrece mayor seguridad por defecto.

Organización: Grupos de 3-4 estudiantes

Producto esperado: Tabla comparativa y presentación oral o escrita de conclusiones.

Duración: 80 minutos

Actividad 4: Elaboración de una guía sencilla para configurar privacidad y seguridad

Objetivo: Crear una guía explicativa para configurar privacidad y seguridad en una red social elegida.

Descripción:

- Cada estudiante elige una red social (puede ser Facebook, Instagram, WhatsApp, etc.).
- Investiga y documenta los pasos necesarios para configurar la privacidad y seguridad.
- Redacta una guía clara y sencilla con lenguaje accesible, incluyendo la importancia de cada ajuste.
- Entrega la guía para revisión del docente y compañeros, recibe retroalimentación y realiza ajustes finales.

Organización: Individual

Producto esperado: Guía escrita con instrucciones y explicaciones claras.

Duración: 120 minutos (puede dividirse en dos sesiones)

Evaluación

Evaluación diagnóstica

Qué se evalúa: Conocimientos previos sobre privacidad y seguridad en redes sociales.

Cómo se evalúa: Cuestionario breve con preguntas de opción múltiple y verdadero/falso sobre conceptos básicos y experiencias previas.

Instrumento sugerido: Test en línea o en papel de 10 preguntas.

Evaluación formativa

Qué se evalúa: Progreso en la exploración y ajuste de configuraciones, análisis comparativo y capacidad para explicar cambios.

Cómo se evalúa: Revisión de listas anotadas, capturas de pantalla de ajustes, tablas comparativas y presentaciones orales.

Instrumento sugerido: Rúbrica que valore precisión, claridad, comprensión y aplicación práctica en cada actividad.

Evaluación sumativa

Qué se evalúa: Capacidad para crear una guía clara y completa para configurar privacidad y seguridad, con explicaciones fundamentadas.

Cómo se evalúa: Revisión detallada del producto final (guía escrita) usando criterios de claridad, exhaustividad, lenguaje adecuado y fundamentación de la importancia de los ajustes.

Instrumento sugerido: Rúbrica de evaluación para guías instruccionales, incluyendo criterios de contenido, forma y coherencia.

Unidad 4: Buenas Prácticas y Responsabilidad Digital

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de identificar y describir comportamientos éticos y responsables en el uso de redes sociales mediante ejemplos prácticos.
- Al finalizar la unidad, el estudiante será capaz de analizar situaciones de conflicto en entornos digitales y proponer estrategias adecuadas para su resolución pacífica.
- Al finalizar la unidad, el estudiante será capaz de reconocer señales de ciberacoso y aplicar medidas preventivas y de respuesta según protocolos establecidos.
- Al finalizar la unidad, el estudiante será capaz de elaborar mensajes digitales que promuevan el respeto y la empatía en sus interacciones en redes sociales.

- Al finalizar la unidad, el estudiante será capaz de evaluar sus propias prácticas en redes sociales y ajustar su comportamiento para fomentar una identidad digital segura y respetuosa.

Contenidos Temáticos

1. Introducción a la Ética y Responsabilidad Digital

- **Concepto de ética digital:** Definición y importancia del comportamiento ético en internet y redes sociales.
- **Responsabilidad en el uso de redes sociales:** Cómo nuestras acciones en línea afectan a otros y a nosotros mismos.
- **Ejemplos prácticos de comportamiento ético:** Casos cotidianos para identificar acciones responsables e irresponsables en redes.

2. Gestión y Resolución de Conflictos en Entornos Digitales

- **Tipos comunes de conflictos en redes sociales:** Malentendidos, discusiones, difamación, etc.
- **Estrategias para la resolución pacífica:** Comunicación asertiva, empatía, mediación y búsqueda de soluciones constructivas.
- **Herramientas y recursos para mediar y resolver conflictos online:** Funciones de bloqueo, reporte, diálogo y apoyo de adultos o autoridades.

3. Ciberacoso: Reconocimiento y Prevención

- **Definición y tipos de ciberacoso:** Insultos, exclusión, difusión de rumores, suplantación, etc.
- **Señales y síntomas del ciberacoso:** Cambios en el comportamiento, aislamiento, ansiedad, etc.
- **Protocolos y medidas preventivas:** Cómo actuar antes, durante y después de un caso de ciberacoso.
- **Recursos de apoyo y denuncia:** Instituciones escolares, familiares y plataformas digitales.

4. Comunicación Responsable: Promoviendo Respeto y Empatía

- **Importancia del respeto y la empatía en mensajes digitales:** Impacto positivo en la comunidad virtual.
- **Elementos de un mensaje respetuoso y empático:** Lenguaje adecuado, tono positivo, escucha activa.
- **Prácticas para mejorar la comunicación digital:** Reflexión antes de publicar, evitar mensajes impulsivos o dañinos.

5. Autoevaluación y Ajuste del Comportamiento en Redes Sociales

- **Reflexión personal sobre el uso de redes sociales:** Identificación de hábitos y actitudes.
- **Herramientas para evaluar la propia identidad digital:** Checklist de comportamientos seguros y responsables.
- **Estrategias para mejorar y mantener una identidad digital positiva:** Ajustes en la privacidad, contenido compartido y relaciones en línea.

Actividades

Actividad 1: Análisis de Casos Éticos en Redes Sociales

Objetivo: Identificar y describir comportamientos éticos y responsables en el uso de redes sociales mediante ejemplos prácticos.

Descripción paso a paso:

- Presentar a los estudiantes varios casos hipotéticos de interacciones en redes sociales (incluyendo ejemplos de comportamiento ético e irresponsable).
- En grupos pequeños, analizar cada caso para identificar qué comportamiento se está mostrando y discutir sus consecuencias.
- Elaborar una lista de acciones responsables y no responsables basadas en los casos.
- Compartir con el grupo clase las conclusiones y reflexionar sobre la importancia de actuar con ética digital.

Organización: Grupos pequeños (3-4 estudiantes)

Producto esperado: Lista de comportamientos éticos e irresponsables con ejemplos y conclusiones compartidas.

Duración estimada: 60 minutos

Actividad 2: Role-Playing para Resolución de Conflictos Digitales

Objetivo: Analizar situaciones de conflicto en entornos digitales y proponer estrategias adecuadas para su resolución pacífica.

Descripción paso a paso:

- Dividir a los estudiantes en parejas o tríos y asignarles un conflicto digital simulado (por ejemplo, malentendidos en comentarios, disputas en grupos, etc.).
- Cada grupo prepara un role-playing donde representan el conflicto y luego practican una resolución pacífica usando estrategias como la comunicación asertiva y la empatía.
- Presentar los role-playing frente a la clase y discutir las soluciones propuestas.
- Reflexionar sobre la importancia de la resolución pacífica y el autocontrol en línea.

Organización: Parejas o tríos

Producto esperado: Presentación de role-playing y plan de resolución de conflicto.

Duración estimada: 70 minutos

Actividad 3: Identificación y Prevención del Ciberacoso

Objetivo: Reconocer señales de ciberacoso y aplicar medidas preventivas y de respuesta según protocolos establecidos.

Descripción paso a paso:

- Mostrar videos o narrar testimonios sobre casos reales de ciberacoso adaptados al nivel.
- Realizar una lluvia de ideas para identificar señales y síntomas del ciberacoso.

- Dividir a los estudiantes en grupos para crear un cartel o infografía con medidas preventivas y protocolos de actuación.
- Compartir los materiales creados con toda la clase y discutir cómo pueden ayudar a protegerse y ayudar a otros.

Organización: Grupos pequeños (3-4 estudiantes)

Producto esperado: Carteles o infografías sobre prevención y respuesta ante el ciberacoso.

Duración estimada: 80 minutos

Actividad 4: Creación de Mensajes Digitales que Promuevan Respeto y Empatía

Objetivo: Elaborar mensajes digitales que promuevan el respeto y la empatía en sus interacciones en redes sociales.

Descripción paso a paso:

- Explicar y analizar ejemplos de mensajes respetuosos y empáticos en redes sociales.
- Indicar pautas para redactar mensajes positivos: lenguaje inclusivo, tono amigable, evitar juicios.
- Cada estudiante redacta al menos tres mensajes que podrían usar en sus redes o grupos escolares para fomentar un ambiente respetuoso.
- Compartir los mensajes con compañeros para recibir retroalimentación y mejorar.

Organización: Individual

Producto esperado: Colección de mensajes digitales con enfoque en respeto y empatía.

Duración estimada: 50 minutos

Actividad 5: Autoevaluación y Plan de Mejora Personal en Redes Sociales

Objetivo: Evaluar sus propias prácticas en redes sociales y ajustar su comportamiento para fomentar una identidad digital segura y respetuosa.

Descripción paso a paso:

- Distribuir un cuestionario o checklist para que cada estudiante evalúe su comportamiento y hábitos en redes sociales (ej.: privacidad, tipo de contenido publicado, interacción con otros).
- Reflexionar individualmente sobre los resultados y detectar áreas de mejora.
- Elaborar un plan personal con al menos tres acciones específicas para mejorar su identidad digital.
- Compartir voluntariamente algunos compromisos con la clase para motivar a otros.

Organización: Individual

Producto esperado: Plan personal de mejora en el uso responsable de redes sociales.

Duración estimada: 60 minutos

Evaluación

Evaluación Diagnóstica

Qué se evalúa: Conocimientos previos sobre ética digital, conflictos en redes, ciberacoso y comportamiento responsable.

Cómo se evalúa: Mediante un cuestionario breve con preguntas de opción múltiple y situaciones hipotéticas para identificar actitudes y conocimientos iniciales.

Instrumento sugerido: Cuestionario escrito o digital (Google Forms, Kahoot) con preguntas sobre conceptos básicos y ejemplos.

Evaluación Formativa

Qué se evalúa: Progreso en la comprensión y aplicación de los contenidos a través de actividades prácticas, reflexión y participación.

Cómo se evalúa: Observación directa durante actividades grupales e individuales, revisión de productos parciales (listas, role-playing, carteles, mensajes, planes personales), y retroalimentación continua.

Instrumento sugerido: Rúbricas específicas para cada actividad que valoren comprensión, análisis, creatividad, y aplicación ética.

Evaluación Sumativa

Qué se evalúa: Capacidad para identificar comportamientos éticos, analizar conflictos, reconocer ciberacoso, elaborar mensajes positivos y autoevaluar su práctica digital.

Cómo se evalúa: Proyecto final individual o en parejas donde el estudiante presenta un portafolio que incluye:

- Ejemplos analizados de comportamiento ético.
- Propuesta de resolución para un conflicto digital.
- Identificación y protocolo ante un caso de ciberacoso.
- Mensajes digitales creados para promover respeto y empatía.
- Autoevaluación y plan de mejora personal.

Instrumento sugerido: Rúbrica de evaluación del portafolio que considere comprensión, análisis crítico, creatividad, y compromiso personal.