

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 comprender y aplicar buenas prácticas de seguridad en el uso de redes sociales. En la actualidad, las redes sociales son plataformas fundamentales para la comunicación y el intercambio de información, pero también representan riesgos significativos para la privacidad y la seguridad personal. Este curso ofrece un enfoque integral para que los jóvenes aprendan a manejar sus datos personales de forma segura y responsable.

El curso está dirigido a estudiantes de 12 a 15 años que usan o desean usar redes sociales de manera informada, promoviendo un ambiente de aprendizaje activo y participativo mediante actividades prácticas, análisis de casos y discusiones grupales. Al finalizar, los estudiantes serán capaces de identificar amenazas comunes en redes sociales, proteger su información personal, reconocer comportamientos riesgosos y aplicar estrategias para un uso seguro y ético de estas plataformas.

Objetivos Generales

- Comprender los conceptos fundamentales de seguridad y privacidad en redes sociales.
- Identificar y evaluar riesgos asociados con el uso de redes sociales en su vida diaria.
- Configurar adecuadamente las opciones de privacidad y seguridad en diversas plataformas.
- Desarrollar habilidades para detectar y responder ante situaciones de ciberacoso y fraudes digitales.
- Promover hábitos digitales responsables y éticos para un uso seguro de las redes sociales.

Competencias

- Identificar riesgos y amenazas comunes en redes sociales para proteger su privacidad.
- Aplicar configuraciones de seguridad y privacidad adecuadas en distintas plataformas sociales.
- Analizar críticamente la información compartida en redes sociales y sus posibles impactos.
- Reconocer y actuar ante situaciones de ciberacoso o conductas inapropiadas en línea.
- Promover un uso responsable, ético y seguro de las redes sociales.

Requerimientos

- Conocimientos básicos en el uso de dispositivos digitales (computadoras, smartphones).
- Acceso a una computadora o dispositivo con conexión a internet para actividades prácticas.

- Cuenta activa en al menos una red social (opcional, para práctica supervisada).
- Material para tomar notas y realizar actividades (cuaderno, lápiz o dispositivo digital).

Unidades del Curso

Unidad 1: Introducción a las Redes Sociales y su Seguridad

Unidad 2: Privacidad y Protección de Datos Personales

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de explicar los conceptos básicos de privacidad y datos personales en redes sociales utilizando ejemplos cotidianos.
- Al finalizar la unidad, el estudiante será capaz de identificar información personal sensible en diferentes tipos de publicaciones y mensajes en plataformas sociales.
- Al finalizar la unidad, el estudiante será capaz de configurar adecuadamente las opciones de privacidad en al menos dos redes sociales populares siguiendo instrucciones paso a paso.
- Al finalizar la unidad, el estudiante será capaz de evaluar riesgos potenciales asociados con compartir datos personales en línea y proponer acciones para minimizar esos riesgos.
- Al finalizar la unidad, el estudiante será capaz de aplicar buenas prácticas para proteger su identidad digital y evitar la exposición innecesaria de información personal en redes sociales.

Contenidos Temáticos

1. Introducción a la Privacidad y Datos Personales en Redes Sociales

- **Concepto de privacidad:** Definición y su importancia en la vida digital.
- **Datos personales:** Qué son, tipos (nombre, dirección, teléfono, fotos, ubicación, etc.) y ejemplos cotidianos.
- **Por qué proteger nuestros datos:** Consecuencias de compartir datos sin cuidado.

2. Identificación de Información Personal Sensible en Publicaciones y Mensajes

- **Ejemplos de información sensible:** Datos que pueden poner en riesgo la privacidad, como números de teléfono, direcciones, fechas de nacimiento, fotos comprometedoras.
- **Tipos de publicaciones y mensajes:** Texto, imágenes, videos, historias y mensajes directos.
- **Reconocimiento de riesgos:** Cómo identificar cuándo una publicación puede exponer información privada.

3. Configuración de Privacidad en Redes Sociales Populares

- **Principios básicos de configuración de privacidad:** Visibilidad de la información, control de publicaciones y lista de amigos.

- **Configuración en Facebook:** Paso a paso para ajustar privacidad de perfil, publicaciones y lista de amigos.
- **Configuración en Instagram:** Cómo proteger la cuenta, controlar quién ve las publicaciones y mensajes.
- **Configuración en otras plataformas (opcional):** Breve introducción a privacidad en WhatsApp o TikTok.

4. Evaluación de Riesgos al Compartir Datos Personales en Línea

- **Tipos de riesgos:** Robo de identidad, ciberacoso, suplantación, fraudes.
- **Ejemplos prácticos:** Situaciones comunes donde se presentan riesgos.
- **Estrategias para minimizar riesgos:** Pensar antes de publicar, verificar configuraciones, no aceptar solicitudes de desconocidos.

5. Buenas Prácticas para Proteger la Identidad Digital

- **Uso de contraseñas seguras:** Cómo crear y gestionar contraseñas.
- **Control de información compartida:** Qué publicar y qué evitar.
- **Gestión de amistades y seguidores:** Selección cuidadosa y revisión periódica.
- **Actualización constante:** Mantener aplicaciones y configuraciones al día.
- **Conciencia y responsabilidad digital:** Actitud frente a la privacidad en redes sociales.

Actividades

Actividad 1: Identificando Datos Personales en Publicaciones

Objetivo: Identificar información personal sensible en diferentes tipos de publicaciones y mensajes.

Descripción:

- El docente presenta ejemplos impresos o digitales de publicaciones y mensajes de redes sociales simuladas.
- Los estudiantes, en parejas, analizan cada ejemplo y subrayan o anotan la información que consideran personal o sensible.
- Discuten en grupo cuáles pueden ser los riesgos de compartir esa información.
- Se realiza una puesta en común donde se contrastan las respuestas y el docente aclara dudas.

Organización: Parejas

Producto esperado: Lista anotada de información sensible en cada ejemplo.

Duración estimada: 40 minutos

Actividad 2: Configurando la Privacidad en Facebook e Instagram

Objetivo: Configurar adecuadamente las opciones de privacidad en al menos dos redes sociales populares siguiendo instrucciones paso a paso.

Descripción:

- El docente proporciona guías impresas o proyectadas con instrucciones para configurar privacidad en Facebook e Instagram.

- Cada estudiante accede a sus cuentas (o a cuentas de práctica si no tienen) y sigue los pasos para ajustar la privacidad.
- Los estudiantes documentan con capturas de pantalla o notas los cambios realizados.
- Se comparte en grupo las dificultades encontradas y las soluciones.

Organización: Individual

Producto esperado: Registro de configuraciones realizadas con evidencia visual o escrita.

Duración estimada: 60 minutos

Actividad 3: Análisis de Riesgos y Propuestas de Protección

Objetivo: Evaluar riesgos potenciales asociados con compartir datos personales en línea y proponer acciones para minimizar esos riesgos.

Descripción:

- Se presenta a los estudiantes diferentes escenarios o casos hipotéticos donde se comparten datos personales en redes sociales.
- En grupos pequeños, analizan los riesgos que cada escenario puede implicar.
- Elaboran una lista de recomendaciones o acciones para evitar esos riesgos.
- Cada grupo expone su análisis y recomendaciones al resto de la clase.

Organización: Grupos de 4-5 estudiantes

Producto esperado: Informe breve con análisis de riesgos y propuestas de protección.

Duración estimada: 50 minutos

Actividad 4: Creando un Manual de Buenas Prácticas para la Identidad Digital

Objetivo: Aplicar buenas prácticas para proteger la identidad digital y evitar la exposición innecesaria de información personal en redes sociales.

Descripción:

- De forma individual, cada estudiante elabora un pequeño manual o cartel digital con consejos y buenas prácticas para cuidar la privacidad y la identidad digital.
- El manual debe incluir al menos 5 recomendaciones claras y ejemplos ilustrativos.
- Se comparten los manuales en clase y se seleccionan algunos para publicar en el aula o en la plataforma digital de la escuela.

Organización: Individual

Producto esperado: Manual o cartel digital de buenas prácticas.

Duración estimada: 70 minutos

Evaluación

Evaluación Diagnóstica

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

Cómo se evalúa: Mediante un cuestionario corto con preguntas abiertas y de opción múltiple sobre conceptos básicos y ejemplos.

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

Evaluación Formativa

Qué se evalúa: Progreso en la identificación de información personal, configuración de privacidad y análisis de riesgos.

Cómo se evalúa: Observación directa durante actividades, revisión de productos parciales (listas, capturas, informes) y retroalimentación continua.

Instrumento sugerido: Rúbrica de evaluación para actividades prácticas y listas de cotejo para participación y comprensión.

Evaluación Sumativa

Qué se evalúa: Comprensión global y aplicación de los conceptos y habilidades de la unidad.

Cómo se evalúa: Elaboración final del manual de buenas prácticas; presentación oral o escrita de análisis de riesgos; prueba escrita con preguntas teóricas y prácticas.

Instrumento sugerido: Rúbrica para manual y presentación, prueba escrita con preguntas de desarrollo y aplicación.

Unidad 3: Identificación y Manejo de Riesgos y Amenazas

Unidad 4: Uso Responsable y Ético de las Redes Sociales