Seguridad Digital y Protección de Datos: Navegando Seguro en el Mundo Digital

Tecnología e Informática | Informática | 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 principios fundamentales para proteger su información y privacidad en el entorno digital. A lo largo de cuatro semanas, los jóvenes aprenderán a identificar riesgos comunes en internet, entender las mejores prácticas de seguridad digital y aplicar medidas para proteger sus datos personales de manera efectiva.

Dirigido a estudiantes de 12 a 15 años, el curso combina teoría con actividades prácticas que fomentan el aprendizaje activo y el pensamiento crítico. Se utilizarán metodologías participativas, que incluyen análisis de casos, simulaciones y proyectos colaborativos, para que los alumnos internalicen los conceptos y desarrollen habilidades para prevenir y resolver problemas relacionados con la seguridad digital.

Al finalizar, los estudiantes estarán capacitados para reconocer amenazas digitales, proteger su información personal, gestionar contraseñas seguras, y adoptar conductas responsables en el uso de tecnologías, promoviendo así un entorno digital seguro y confiable en su vida cotidiana.

Objetivos Generales

- Reconocer y describir las principales amenazas y vulnerabilidades en el entorno digital.
- Implementar estrategias básicas para proteger la información personal y la privacidad en línea.
- Evaluar diferentes situaciones de riesgo digital y seleccionar medidas preventivas adecuadas.
- Promover hábitos seguros y responsables en el uso cotidiano de tecnologías digitales.

Competencias

- Identificar riesgos y amenazas comunes en el entorno digital que afectan la seguridad y privacidad.
- Aplicar técnicas básicas para proteger datos personales y contraseñas en diversas plataformas digitales.
- Analizar situaciones problemáticas relacionadas con la seguridad digital y proponer soluciones adecuadas.
- Demostrar responsabilidad y buenas prácticas en el uso de dispositivos y redes digitales.
- Utilizar herramientas básicas para gestionar la privacidad y seguridad en redes sociales y aplicaciones.

Requerimientos

- Conocimientos básicos de uso de computadoras y navegación por internet.

- Acceso a una computadora o dispositivo móvil con conexión a internet.
- Cuenta de correo electrónico activa para actividades prácticas.
- Material para tomar apuntes y realizar actividades (cuaderno, lápiz o dispositivo digital).

Unidades del Curso

Unidad 1: Introducción a la Seguridad Digital

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de definir conceptos básicos de seguridad digital y explicar su importancia en el entorno en línea.
- Al finalizar la unidad, el estudiante será capaz de identificar los tipos comunes de amenazas digitales que afectan a los usuarios de internet.
- Al finalizar la unidad, el estudiante será capaz de describir las consecuencias de no proteger la información personal en plataformas digitales.
- Al finalizar la unidad, el estudiante será capaz de reconocer prácticas inseguras en el uso diario de tecnologías digitales y justificar la necesidad de evitarlas.
- Al finalizar la unidad, el estudiante será capaz de clasificar diferentes riesgos digitales y asociarlos con las vulnerabilidades que los originan.

Contenidos Temáticos

1. Conceptos básicos de seguridad digital

- **Definición de seguridad digital:** Explicación sencilla de qué es la seguridad digital, su propósito y su importancia para proteger la información y la privacidad en el entorno digital.
- **Elementos clave de la seguridad digital:** Confidencialidad, integridad y disponibilidad de la información.
- **Ejemplos cotidianos:** Situaciones comunes donde la seguridad digital es relevante, como el uso de redes sociales, correo electrónico y plataformas educativas.

2. Tipos comunes de amenazas digitales

- **Malware:** Virus, troyanos, ransomware y spyware: qué son y cómo afectan a los dispositivos y la información.
- **Phishing:** Definición, cómo identificar correos y mensajes falsos que buscan robar información personal.
- **Suplantación de identidad (spoofing):** Explicación y ejemplos de cómo alguien puede hacerse pasar por otra persona en línea.
- **Contraseñas débiles y robo de credenciales:** Riesgos y métodos que usan los atacantes para acceder a cuentas.

3. Consecuencias de no proteger la información personal

- **Pérdida de privacidad:** Cómo la información personal puede ser utilizada sin consentimiento.
- **Riesgo de fraude y robo de identidad:** Ejemplos de cómo los datos personales pueden ser usados para cometer delitos.
- **Daño a la reputación digital:** Impacto de la exposición pública no deseada en redes sociales y otras plataformas.
- **Problemas legales y financieros:** Consecuencias de compartir o perder datos sensibles.

4. Prácticas inseguras en el uso diario de tecnologías digitales

- **Uso de contraseñas fáciles de adivinar o repetidas:** Ejemplos y riesgos.
- **Acceso a redes Wi-Fi públicas sin medidas de seguridad:** Peligros y consejos para evitarlos.
- **Compartir información personal en exceso en redes sociales:** Riesgos asociados.
- **No actualizar software y aplicaciones:** Cómo esto puede abrir vulnerabilidades.

5. Clasificación de riesgos digitales y sus vulnerabilidades

- **Riesgos técnicos:** Vulnerabilidades en software, hardware y redes.
- **Riesgos humanos:** Errores, descuidos y comportamiento inseguro.
- **Riesgos externos:** Ataques de ciberdelincuentes, hacktivismo, etc.
- **Ejemplos prácticos:** Asociar cada riesgo con las vulnerabilidades que lo originan para facilitar la comprensión.

Actividades

Actividad 1: Mapa conceptual sobre seguridad digital

Objetivo: Definir conceptos básicos de seguridad digital y explicar su importancia.

Descripción:

- El docente presenta el tema y los conceptos clave.
- Los estudiantes, en parejas, crean un mapa conceptual que incluya definición, elementos y ejemplos de seguridad digital.
- Se comparten los mapas en plenaria para retroalimentación.

Organización: Parejas

Producto esperado: Mapa conceptual digital o en papel.

Duración estimada: 50 minutos

Actividad 2: Análisis de casos de amenazas digitales

Objetivo: Identificar tipos comunes de amenazas digitales que afectan a usuarios.

Descripción:

- El docente presenta varios casos o noticias breves sobre ataques digitales.
- En grupos de 3-4 estudiantes, analizan cada caso para identificar el tipo de amenaza digital involucrada.

- Discuten medidas que podrían tomarse para evitar esos riesgos.
- Cada grupo expone un caso resumido y sus conclusiones.

Organización: Grupos de 3-4 estudiantes

Producto esperado: Presentación oral o cartel resumen

Duración estimada: 60 minutos

Actividad 3: Debate sobre prácticas inseguras y consecuencias

Objetivo: Reconocer prácticas inseguras y justificar la necesidad de evitarlas; describir consecuencias de no proteger la información.

Descripción:

- Se propone una lista de prácticas inseguras comunes.
- Los estudiantes forman dos equipos: uno defiende por qué algunas personas usan esas prácticas y el otro argumenta por qué son riesgosas y deben evitarse.
- Después del debate, el docente guía una reflexión sobre las consecuencias reales de no proteger la información personal.

Organización: Grupos grandes (dos equipos)

Producto esperado: Argumentos escritos y conclusiones compartidas

Duración estimada: 45 minutos

Actividad 4: Clasificación de riesgos y vulnerabilidades

Objetivo: Clasificar riesgos digitales y asociarlos con sus vulnerabilidades.

Descripción:

- El docente entrega tarjetas con diferentes riesgos digitales y otras con vulnerabilidades.
- En grupos, los estudiantes deben emparejar riesgos con las vulnerabilidades que los originan y justificar su elección.
- Finalmente, cada grupo explica sus asociaciones ante la clase.

Organización: Grupos de 3 estudiantes

Producto esperado: Tabla o listado con riesgo y vulnerabilidad asociada

Duración estimada: 40 minutos

Evaluación

Evaluación diagnóstica

Qué se evalúa: Conocimientos previos sobre seguridad digital, amenazas y prácticas en internet.

Cómo se evalúa: Cuestionario breve con preguntas abiertas y de opción múltiple para conocer ideas previas.

Instrumento sugerido: Formulario impreso o digital con 5-7 preguntas básicas.

Evaluación formativa

Qué se evalúa: Participación y comprensión durante las actividades, análisis de casos y debates.

Cómo se evalúa: Observación directa del docente, revisión de productos parciales (mapas conceptuales, presentaciones, tablas).

Instrumento sugerido: Lista de cotejo para evaluar participación, relevancia de aportes y calidad de productos.

Evaluación sumativa

Qué se evalúa: Capacidad para definir conceptos, identificar amenazas, describir consecuencias, reconocer prácticas inseguras y clasificar riesgos con sus vulnerabilidades.

Cómo se evalúa: Prueba escrita con preguntas de definición, análisis de casos, preguntas de clasificación y justificación de respuestas.

Instrumento sugerido: Examen con preguntas de desarrollo, selección múltiple y casos cortos para análisis.

Unidad 2: Amenazas y Riesgos en el Mundo Digital

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de identificar diferentes tipos de amenazas digitales, como virus, malware, phishing y ciberacoso, mediante ejemplos concretos.
- Al finalizar la unidad, el estudiante será capaz de describir cómo las amenazas digitales afectan la seguridad de sus datos personales en situaciones cotidianas.
- Al finalizar la unidad, el estudiante será capaz de clasificar distintos riesgos digitales según su nivel de peligro y frecuencia de ocurrencia en ambientes escolares y sociales.
- Al finalizar la unidad, el estudiante será capaz de analizar casos prácticos de ataques digitales y explicar las consecuencias para la privacidad y seguridad de la información.
- Al finalizar la unidad, el estudiante será capaz de recomendar medidas básicas para prevenir y protegerse de amenazas digitales, justificando la importancia de cada una.

Contenidos Temáticos

1. Introducción a las Amenazas y Riesgos en el Mundo Digital

- Concepto de amenazas digitales: definición y ejemplos básicos.
- Diferencia entre amenaza y riesgo digital.
- Importancia de la seguridad digital en la vida cotidiana de los jóvenes.

2. Tipos de Amenazas Digitales

- Virus y Malware
  - Definición y características.

    - Cómo se propagan y ejemplos comunes.
    - Impacto en dispositivos y datos personales.
- Phishing
    - Definición y objetivos.
    - Ejemplos de correos, mensajes o páginas falsas.
    - Cómo detectar intentos de phishing.
- Ciberacoso
    - Qué es el ciberacoso y cómo se manifiesta.
    - Diferencia entre acoso tradicional y digital.
    - Consecuencias emocionales y legales.
- Otras amenazas comunes
    - Spyware, ransomware y adware: definiciones y efectos.
    - Spam y su relación con riesgos de seguridad.

3. Impacto de las Amenazas Digitales en la Seguridad de Datos Personales

- Cómo las amenazas digitales pueden comprometer datos personales (ejemplos cotidianos).
- Riesgos de compartir información sin precaución en redes sociales y aplicaciones.
- Ejemplos de consecuencias reales: pérdida de información, suplantación de identidad, daño reputacional.

4. Clasificación de Riesgos Digitales

- Criterios para clasificar riesgos: nivel de peligro y frecuencia de ocurrencia.
- Clasificación de riesgos en ambientes escolares (ejemplos: uso de dispositivos en clase, redes escolares).
- Clasificación de riesgos en ambientes sociales (ejemplos: redes sociales, juegos en línea).
- Discusión sobre riesgos emergentes y su evolución.

5. Análisis de Casos Prácticos de Ataques Digitales

- Presentación de casos reales o simulados de ataques digitales.
- Identificación de la amenaza involucrada y las vulnerabilidades explotadas.
- Consecuencias para la privacidad y la seguridad de la información.
- Reflexión sobre lecciones aprendidas y posibles respuestas.

6. Medidas Básicas para Prevenir y Protegerse de Amenazas Digitales

- Buenas prácticas para la protección de datos personales: contraseñas, actualizaciones y copias de seguridad.
- Uso seguro de correos electrónicos y redes sociales para evitar phishing y ciberacoso.
- Importancia del software antivirus y antimalware.
- Cómo reportar y buscar ayuda ante incidentes digitales.

- Justificación de la importancia de cada medida para la seguridad personal y colectiva.

Actividades

Actividad 1: Identificando Amenazas Digitales en Ejemplos Reales

Objetivo: Contribuye a identificar diferentes tipos de amenazas digitales mediante ejemplos concretos.

Descripción:

- El docente presenta una serie de ejemplos breves (videos, imágenes o textos) que muestran situaciones con virus, phishing, ciberacoso y malware.
- Los estudiantes, en grupos pequeños, analizan cada ejemplo y determinan qué tipo de amenaza digital representa.
- Discusión grupal para validar las respuestas y aclarar dudas.

Organización: Grupos de 3-4 estudiantes.

Producto esperado: Lista con ejemplos y clasificación correcta de la amenaza digital.

Duración estimada: 45 minutos.

Actividad 2: Simulación de un Ataque de Phishing

Objetivo: Describir cómo las amenazas digitales afectan la seguridad de datos personales en situaciones cotidianas.

Descripción:

- El docente presenta un correo electrónico simulado que intenta engañar para obtener datos personales (phishing).
- Individualmente, cada estudiante identifica señales de alerta en el correo y explica qué información podría estar en riesgo.
- Se realiza una plenaria para reflexionar y establecer recomendaciones para evitar caer en phishing.

Organización: Individual con discusión grupal.

Producto esperado: Lista de señales de alerta y breve explicación de riesgos.

Duración estimada: 30 minutos.

Actividad 3: Clasificación de Riesgos Digitales en el Entorno Escolar y Social

Objetivo: Clasificar riesgos digitales según nivel de peligro y frecuencia en ambientes escolares y sociales.

Descripción:

- Se entregan a los estudiantes tarjetas con diferentes riesgos digitales descritos.
- En parejas, organizan las tarjetas en un cuadro de doble entrada con criterios: "Nivel de Peligro" (Alto, Medio, Bajo) y "Frecuencia de Ocurrencia" (Frecuente, Poco frecuente, Raro).
- Presentan su cuadro y justifican su clasificación ante el grupo.

Organización: Parejas.

Producto esperado: Cuadro de clasificación y justificación oral.

Duración estimada: 40 minutos.

Actividad 4: Análisis y Propuesta de Prevención ante un Caso de Ciberataque

Objetivo: Analizar casos prácticos de ataques digitales y recomendar medidas básicas para prevenirlos, justificando su importancia.

Descripción:

- Se presenta un caso práctico (real o ficticio) de un ciberataque que afectó a un usuario o grupo.
- En grupos, los estudiantes analizan: qué amenaza fue, cómo ocurrió, consecuencias para la privacidad y seguridad.
- Desarrollan un listado de medidas preventivas que podrían haber evitado el ataque, con explicación de la importancia de cada medida.
- Cada grupo presenta su análisis y recomendaciones.

Organización: Grupos de 4 estudiantes.

Producto esperado: Informe escrito y presentación oral del análisis y medidas preventivas.

Duración estimada: 60 minutos.

Evaluación

Evaluación Diagnóstica

Qué se evalúa: Conocimientos previos sobre amenazas digitales y riesgos asociados.

Cómo se evalúa: Cuestionario corto con preguntas de opción múltiple y preguntas abiertas sobre amenazas conocidas.

Instrumento sugerido: Test escrito o digital (5-7 preguntas).

Evaluación Formativa

Qué se evalúa: Progreso en la identificación, clasificación y análisis de amenazas digitales durante las actividades.

Cómo se evalúa: Observación directa, revisión de productos de actividades (listas, cuadros, análisis) y participación en discusiones.

Instrumento sugerido: Rúbrica de desempeño para actividades grupales e individuales.

Evaluación Sumativa

Qué se evalúa: Competencia para identificar amenazas, describir su impacto, clasificar riesgos, analizar casos y proponer medidas preventivas.

Cómo se evalúa: Examen escrito con preguntas de desarrollo y análisis de un caso práctico, además de evaluación del informe y presentación de la actividad 4.

Instrumento sugerido: Examen escrito y rúbrica para evaluación de informe y presentación oral.

Unidad 3: Protección de Datos Personales y Privacidad

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de crear y gestionar contraseñas seguras aplicando buenas prácticas reconocidas para proteger su información personal.
- Al finalizar la unidad, el estudiante será capaz de configurar adecuadamente las opciones de privacidad en redes sociales para controlar quién puede acceder a su información personal.
- Al finalizar la unidad, el estudiante será capaz de identificar y evaluar los permisos solicitados por aplicaciones móviles para tomar decisiones responsables sobre su uso.
- Al finalizar la unidad, el estudiante será capaz de explicar la importancia de proteger los datos personales y cómo estas acciones contribuyen a mantener la privacidad en el entorno digital.
- Al finalizar la unidad, el estudiante será capaz de aplicar estrategias básicas para evitar compartir información sensible en línea, promoviendo hábitos seguros en el uso cotidiano de tecnologías digitales.

Contenidos Temáticos

1. Introducción a la Protección de Datos Personales y Privacidad

- **¿Qué son los datos personales?** Concepto de datos personales y ejemplos comunes en la vida diaria.
- **Importancia de la privacidad en el entorno digital** Por qué proteger nuestros datos es fundamental para nuestra seguridad y bienestar.
- **Riesgos asociados a la exposición de datos personales** Consecuencias de compartir información sensible sin precaución.

2. Creación y Gestión de Contraseñas Seguras

- **Características de una contraseña segura** Longitud, complejidad, uso de caracteres especiales, evitar información personal.
- **Buenas prácticas para crear contraseñas** Uso de frases clave, combinación de letras, números y símbolos.
- **Gestión y almacenamiento seguro de contraseñas** No reutilizar contraseñas, uso de gestores de contraseñas, actualización periódica.

3. Configuración de Privacidad en Redes Sociales

- **Opciones básicas de privacidad en plataformas comunes** Facebook, Instagram, TikTok, WhatsApp.
- **Control de quién puede ver la información personal** Ajustes para limitar el acceso a publicaciones, fotos y datos personales.
- **Reconocimiento y gestión de solicitudes de amistad y mensajes** Cómo identificar contactos seguros y evitar interacciones riesgosas.

4. Evaluación y Gestión de Permisos en Aplicaciones Móviles

- **Tipos de permisos solicitados por las aplicaciones** Acceso a cámara, micrófono, ubicación, contactos, almacenamiento.
- **Cómo evaluar la necesidad de los permisos** Identificar permisos esenciales versus permisos innecesarios o invasivos.
- **Configuración y revocación de permisos** Pasos para modificar o retirar permisos en dispositivos Android e iOS.

5. Estrategias para Evitar Compartir Información Sensible en Línea

- **Identificación de información sensible** Datos que no deben compartirse públicamente (dirección, teléfono, contraseñas, ubicación en tiempo real).
- **Buenas prácticas para compartir contenido en línea** Reflexionar antes de publicar, uso de configuraciones de privacidad, evitar datos personales en fotos y videos.
- **Reconocimiento y prevención del oversharing (exceso de información)** Consecuencias y cómo evitarlo.

6. Resumen y Reflexión sobre la Protección de Datos Personales

- **Importancia de mantener hábitos seguros en el uso diario** Integración de lo aprendido en la rutina digital.
- **Impacto de la protección de datos en la vida personal y social** Cómo contribuye a una experiencia digital segura y confiable.

Actividades

Actividad 1: Creando Contraseñas Seguras

Objetivo: Crear y gestionar contraseñas seguras aplicando buenas prácticas reconocidas para proteger información personal.

Descripción:

- El docente explica las características de una contraseña segura.
- Los estudiantes individualmente crean 3 contraseñas para diferentes cuentas (correo, red social, juego en línea) siguiendo las recomendaciones.
- En parejas, intercambian sus contraseñas para evaluarlas según criterios de seguridad y proponen mejoras.
- Discusión grupal sobre la importancia de no reutilizar contraseñas y cómo recordarlas de forma segura.

Organización: Individual y en parejas

Producto esperado: Lista de contraseñas seguras y evaluación escrita con mejoras sugeridas.

Duración estimada: 45 minutos

Actividad 2: Configura tu Privacidad en Redes Sociales

Objetivo: Configurar adecuadamente las opciones de privacidad en redes sociales para controlar quién accede a la información personal.

Descripción:

- El docente presenta una guía con los ajustes básicos de privacidad en plataformas populares.
- Los estudiantes, en grupos pequeños, seleccionan una red social y simulan configurar un perfil restringiendo el acceso a información personal, amigos y publicaciones.
- Cada grupo presenta sus configuraciones y explica sus decisiones.
- Debate sobre la importancia de estos ajustes y riesgos de no configurarlos.

Organización: Grupos

Producto esperado: Simulación de configuración de privacidad con justificación escrita o verbal.

Duración estimada: 60 minutos

Actividad 3: Análisis de Permisos de Aplicaciones

Objetivo: Identificar y evaluar los permisos solicitados por aplicaciones móviles para tomar decisiones responsables sobre su uso.

Descripción:

- El docente explica los tipos de permisos comunes y su función.
- En parejas, los estudiantes analizan ejemplos reales o ficticios de solicitudes de permisos de diferentes apps.
- Discuten cuáles permisos son necesarios y cuáles podrían ser un riesgo o invasivos.
- Proponen recomendaciones para el uso responsable y seguridad.

Organización: Parejas

Producto esperado: Lista evaluativa de permisos con justificaciones y recomendaciones.

Duración estimada: 45 minutos

Actividad 4: Juego de Roles - Decidiendo qué Compartir

Objetivo: Aplicar estrategias básicas para evitar compartir información sensible en línea, promoviendo hábitos seguros.

Descripción:

- El docente presenta diferentes situaciones o escenarios donde se debe decidir qué información compartir en línea.
- En grupos, los estudiantes representan un diálogo o debate donde uno quiere compartir información sensible y otro explica riesgos y alternativas.
- Cada grupo expone su escena y se reflexiona sobre las mejores prácticas para proteger la privacidad.

Organización: Grupos

Producto esperado: Presentación de role plays y lista de estrategias para compartir información segura.

Duración estimada: 60 minutos

Evaluación

Evaluación Diagnóstica

Qué se evalúa: Conocimientos previos sobre protección de datos, contraseñas, privacidad en redes sociales y permisos de aplicaciones.

Cómo se evalúa: Cuestionario breve con preguntas de opción múltiple y preguntas abiertas sobre hábitos digitales actuales.

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

Evaluación Formativa

Qué se evalúa: Progreso en la creación de contraseñas seguras, configuraciones de privacidad, análisis de permisos y aplicación de estrategias para compartir información.

Cómo se evalúa: Revisión continua de las actividades prácticas, retroalimentación oral y escrita durante las actividades de aprendizaje.

Instrumento sugerido: Rúbrica para evaluar actividades prácticas y participación en debates y role plays.

Evaluación Sumativa

Qué se evalúa: Competencia para crear contraseñas seguras, configurar privacidad, evaluar permisos, explicar la importancia de la protección de datos y aplicar estrategias para evitar compartir información sensible.

Cómo se evalúa: Proyecto final individual que incluya:

- Diseño de contraseñas para diferentes cuentas con justificación.
- Simulación de configuración de privacidad en una red social.
- Análisis crítico de permisos de una aplicación móvil.
- Ensayo breve explicando la importancia de la protección de datos personales.
- Lista de estrategias para evitar compartir información sensible en línea.

Instrumento sugerido: Rúbrica detallada para evaluar el proyecto integrador.

Unidad 4: Prevención y Solución de Problemas de Seguridad Digital

Objetivos de Aprendizaje

- Al finalizar la unidad, el estudiante será capaz de identificar y describir incidentes comunes de seguridad digital mediante el análisis de casos prácticos.
- Al finalizar la unidad, el estudiante será capaz de aplicar medidas preventivas básicas para proteger la información personal en dispositivos digitales en actividades simuladas.
- Al finalizar la unidad, el estudiante será capaz de evaluar situaciones de riesgo digital y seleccionar soluciones adecuadas para resolver problemas de seguridad en entornos virtuales controlados.
- Al finalizar la unidad, el estudiante será capaz de elaborar un plan personal de hábitos seguros y responsables para el uso diario de tecnologías digitales, justificando sus elecciones.

Contenidos Temáticos

1. Introducción a los Incidentes Comunes de Seguridad Digital

- Definición y ejemplos de incidentes comunes: virus, phishing, malware, ransomware, robo de identidad.
- Impacto de los incidentes en la vida personal y escolar.
- Importancia de reconocer señales de alerta en dispositivos y cuentas digitales.

2. Medidas Preventivas Básicas para la Protección de la Información Personal

- Contraseñas seguras: características y gestión responsable.
- Configuración de privacidad en redes sociales y aplicaciones.
- Uso correcto de antivirus y actualizaciones de software.
- Precauciones al descargar archivos y abrir enlaces.

3. Evaluación y Solución de Situaciones de Riesgo Digital

- Identificación de situaciones de riesgo mediante análisis de escenarios.
- Pasos para responder ante un incidente de seguridad digital.
- Herramientas y recursos para solucionar problemas (restauración, reportes, ayuda técnica).
- Importancia de mantener la calma y actuar de manera responsable.

4. Elaboración de un Plan Personal de Hábitos Seguros y Responsables

- Reflexión sobre los hábitos actuales de uso de tecnología.
- Selección de prácticas seguras para proteger la información y la privacidad.
- Justificación de las elecciones en el plan personal.
- Compromiso personal y seguimiento del plan en la vida diaria.

Actividades

Actividad 1: Análisis de Casos Prácticos de Incidentes de Seguridad Digital

Objetivo: Identificar y describir incidentes comunes de seguridad digital mediante el análisis de casos prácticos.

Descripción:

- Presentar a los estudiantes varios casos breves que describen incidentes digitales comunes (p.ej., un correo de phishing recibido, un dispositivo infectado con malware).
- En grupos pequeños, los estudiantes analizan cada caso para identificar qué tipo de incidente es, cómo ocurrió y qué consecuencias tuvo.
- Cada grupo comparte sus conclusiones con el resto de la clase.

Organización: Grupos de 3-4 estudiantes.

Producto esperado: Informe grupal breve que describa los incidentes analizados y sus características.

Duración: 1 hora.

Actividad 2: Simulación de Aplicación de Medidas Preventivas

Objetivo: Aplicar medidas preventivas básicas para proteger la información personal en dispositivos digitales.

Descripción:

- En un entorno controlado (laboratorio o simulador digital), los estudiantes configuran contraseñas seguras, ajustan configuraciones de privacidad y practican la instalación y actualización de antivirus.
- Se presentan situaciones simuladas donde deben decidir si abrir un enlace o descargar un archivo, explicando su elección.

Organización: Individual o parejas.

Producto esperado: Registro de configuraciones realizadas y respuestas justificadas a las situaciones simuladas.

Duración: 1.5 horas.

Actividad 3: Taller de Resolución de Problemas de Seguridad Digital

Objetivo: Evaluar situaciones de riesgo digital y seleccionar soluciones adecuadas para resolver problemas de seguridad.

Descripción:

- Se presentan escenarios con problemas de seguridad digital (p.ej., cuenta hackeada, dispositivo bloqueado por ransomware).
- En equipos, los estudiantes analizan el escenario, identifican riesgos y proponen un plan de acción para resolverlo.
- Discusión grupal para comparar soluciones y reforzar buenas prácticas.

Organización: Grupos de 3-4 estudiantes.

Producto esperado: Plan de acción escrito para cada escenario presentado.

Duración: 1.5 horas.

Actividad 4: Creación de un Plan Personal de Hábitos Seguros y Responsables

Objetivo: Elaborar un plan personal de hábitos seguros y responsables para el uso diario de tecnologías digitales, justificando sus elecciones.

Descripción:

- Reflexión guiada sobre los hábitos actuales de uso de tecnología y posibles riesgos.
- Los estudiantes diseñan un plan personal que incluya prácticas para proteger su información, cuidar su privacidad y utilizar la tecnología de forma responsable.
- Justifican por escrito cada hábito propuesto explicando su importancia.
- Presentación voluntaria del plan a la clase para recibir retroalimentación.

Organización: Individual.

Producto esperado: Documento personal con el plan de hábitos y justificación.

Duración: 2 horas.

Evaluación

Evaluación Diagnóstica

Qué se evalúa: Conocimientos previos sobre incidentes de seguridad digital y hábitos de protección.

Cómo se evalúa: Cuestionario breve con preguntas de opción múltiple y preguntas abiertas sobre experiencias y conocimientos previos.

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

Evaluación Formativa

Qué se evalúa: Progreso en el análisis de casos, aplicación de medidas preventivas y capacidad para resolver problemas de seguridad.

Cómo se evalúa: Revisión continua de productos de actividades (informes, registros de simulación, planes de acción) y observación del desempeño en discusiones y talleres.

Instrumento sugerido: Rúbrica que valore comprensión, aplicación práctica y argumentación en las actividades.

Evaluación Sumativa

Qué se evalúa: Capacidad para identificar incidentes, aplicar medidas preventivas, evaluar riesgos y elaborar un plan personal de hábitos seguros.

Cómo se evalúa: Trabajo final que incluya:

- Análisis de un nuevo caso de incidente digital.
- Simulación o descripción de medidas preventivas aplicadas.
- Propuesta escrita de solución para un problema de seguridad planteado.
- Plan personal de hábitos seguros con justificación.

Instrumento sugerido: Rúbrica detallada con criterios para evaluar cada componente del trabajo final.